






Binding information for IP media flows**Patent number:** JP2004533160T**Publication date:** 2004-10-28**Inventor:****Applicant:****Classification:****- International:** *H04L12/56; H04L29/06; H04Q7/22; H04L12/56; H04L29/06; H04Q7/22; (IPC1-7): H04L12/56; H04Q7/36; H04Q7/38***- european:** H04L12/56B; H04L12/56D; H04L12/56D5; H04L29/06C6C; H04W6/06; H04W36/02**Application number:** JP20020582649T 20020416**Priority number(s):** US20010284358P 20010417; US20020091047 20020304; WO2002US12181 20020416**Also published as:** WO02085055 (A3)
 WO02085055 (A2)
 EP1382214 (A3)
 EP1382214 (A2)
 US2002184510 (A1)

more >>

[Report a data error here](#)

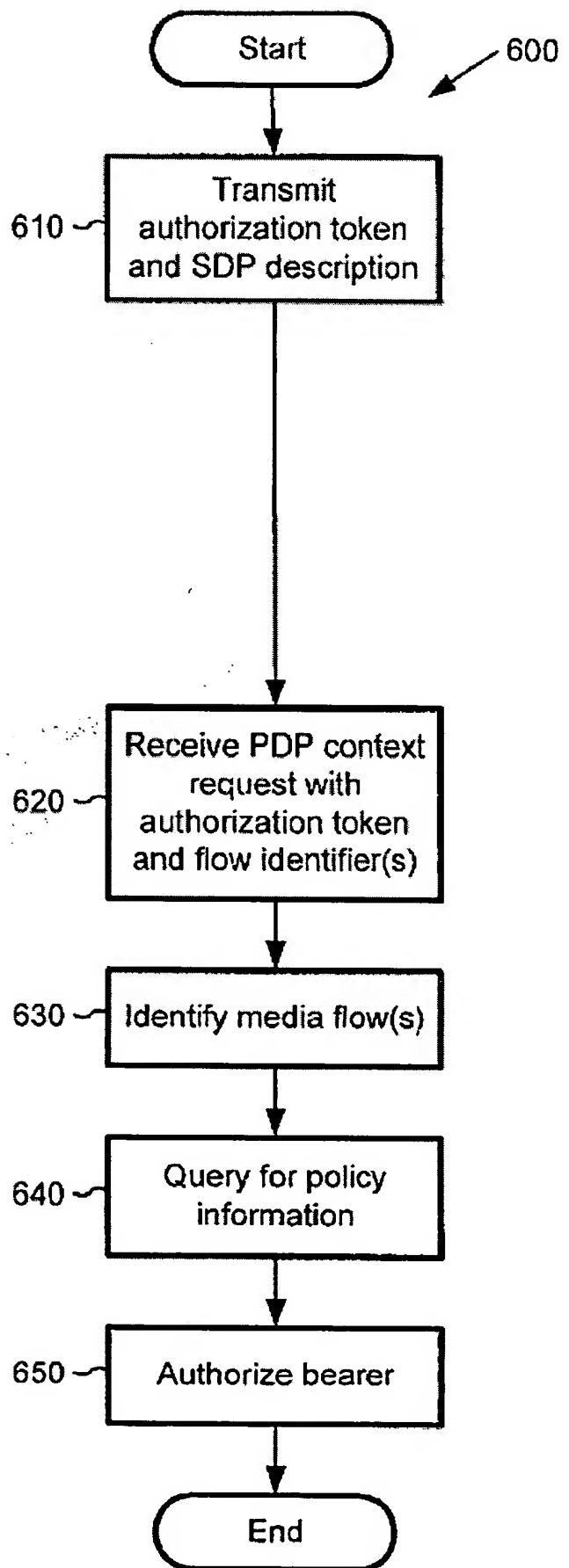
Abstract not available for JP2004533160T

Abstract of corresponding document: **US2002184510**

A binding mechanism uses an authorization token and packet media flow identifier(s) to identify packet media flow(s) of a session for authorization. This provides the advantages of using a per-session authorization token while also allowing resource authorization and allocation on the basis of individual packet media flows of the session. The binding mechanism includes various aspects.

~~THIS PAGE DELETED (USPTO)~~

THIS PAGE BLANK (USPTO)



THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2004-533160

(P2004-533160A)

(43) 公表日 平成16年10月28日 (2004. 10. 28)

(51) Int. Cl. ⁷

F I

テーマコード (参考)

H04L 12/56

H04L 12/56 200A

5K030

H04Q 7/38

H04B 7/26 109M

5K067

H04Q 7/38

H04B 7/26 105D

審査請求 未請求 予備審査請求 有 (全 50 頁)

(21) 出願番号 特願2002-582649 (P2002-582649)
 (86) (22) 出願日 平成14年4月16日 (2002. 4. 16)
 (85) 翻訳文提出日 平成15年10月17日 (2003. 10. 17)
 (86) 国際出願番号 PCT/US2002/012181
 (87) 国際公開番号 W02002/085055
 (87) 国際公開日 平成14年10月24日 (2002. 10. 24)
 (31) 優先権主張番号 60/284, 358
 (32) 優先日 平成13年4月17日 (2001. 4. 17)
 (33) 優先権主張国 米国 (US)
 (31) 優先権主張番号 10/091, 047
 (32) 優先日 平成14年3月4日 (2002. 3. 4)
 (33) 優先権主張国 米国 (US)

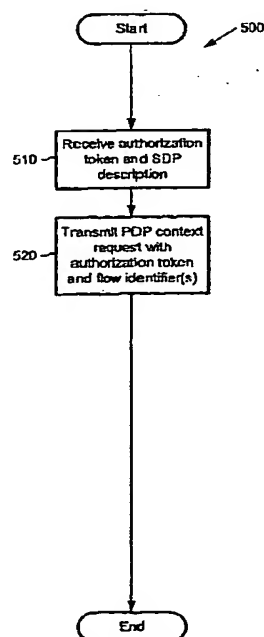
(71) 出願人 502322109
 エイ ティ アンド ティ ワイヤレス
 サービスズ インコーポレイテッド
 アメリカ合衆国ワシントン州, レドモンド
 , ワンハンドレッドシックスティフォース
 ・アベニュー 7277
 (74) 代理人 100089705
 弁理士 社本 一夫
 (74) 代理人 100076691
 弁理士 増井 忠式
 (74) 代理人 100075270
 弁理士 小林 泰
 (74) 代理人 100080137
 弁理士 千葉 昭男

最終頁に続く

(54) 【発明の名称】 IPメディア・フローのためのバインド情報

(57) 【要約】

セッションの1つ以上のメディア・フローを特定し許可するバインド機構を提供する。バインド情報は、許可トークンおよび1つ以上のバケット・メディア・フロー識別子を用いて、許可のためにセッションの1つ以上のバケット・メディア・フローを特定する。これによって、セッションの個々のバケット・メディア・フローに基づいてリソースの許可および配分を可能にしつつも、セッション毎の許可トークンを用いるという利点が得られる。バインド機構は種々の態様を含む。



【特許請求の範囲】**【請求項 1】**

装置において、リソース許可を要求する方法であって、セッションの1つ以上のIPメディア・フローについてのバインド情報を含む1つ以上のPDPコンテキスト要求を送信するステップから成り、前記バインド情報が、許可トークンと、1つ以上のIPメディア・フロー識別子とを含む、方法。

【請求項 2】

請求項1記載の方法において、前記1つ以上のIPメディア・フロー識別子は、前記許可トークンと組み合わせて、前記1つ以上のIPメディア・フローを特定する、方法。

【請求項 3】

請求項1記載の方法において、前記装置はユーザ機器であり、前記1つ以上のIPメディア・フロー識別子は、前記ユーザ機器およびP-CSCF/PCFにアクセス可能なSDP記述におけるフローの順序を参照する、方法。

【請求項 4】

請求項1記載の方法において、各PDPコンテキスト要求は、PDPコンテキスト活性化要求またはPDPコンテキスト変更要求である、方法。

【請求項 5】

コンピュータ実行可能命令がエンコードされたコンピュータ読み取り可能媒体であって、これによってプログラムされたコンピュータに、請求項1記載の方法を実行させる、コンピュータ読み取り可能媒体。

【請求項 6】

ネットワーク・ノードにおいて、リソースを許可する方法であって、セッションの1つ以上のIPメディア・フローについてのバインド情報を処理するステップから成り、前記バインド情報が、許可トークンと、1つ以上のIPメディア・フロー識別子とを含む、方法。

【請求項 7】

請求項6記載の方法において、前記1つ以上のIPメディア・フロー識別子は、前記許可トークンと組み合わせて、前記1つ以上のIPメディア・フローを特定する、方法。

【請求項 8】

請求項6記載の方法において、前記ネットワーク・ノードはP-CSCF/PCFを備え、前記1つ以上のIPメディア・フロー識別子は、前記P-CSCF/PCFおよびユーザ機器にアクセス可能なSDP記述におけるフローの順序を参照する、方法。

【請求項 9】

請求項6記載の方法において、前記処理するステップは、サービスに基づく個別ポリシー判断に応じて前記1つ以上のIPメディア・フローを許可することから成る、方法。

【請求項 10】

コンピュータ実行可能命令がエンコードされたコンピュータ読み取り可能媒体であって、これによってプログラムされたコンピュータに、請求項6記載の方法を実行させる、コンピュータ読み取り可能媒体。

【請求項 11】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたユーザ機器に、リソース許可および配分を要求する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

メディア許可トークンを受信するステップと、セッションの1つ以上のメディア・フローの各々を許可するための前記メディア許可トークンを含むコンテキスト活性化要求を送信するステップと、から成り、前記メディア許可トークンと、複数のメディア・フロー識別子からのメディア・フロー識別子との組み合わせが、前記セッションの複数のメディア・フローの中からメディア・フローを一意に特定するのに十分である、コンピュータ読み取り可能媒体。

【請求項 12】

請求項 1 1 記載のコンピュータ読み取り可能媒体において、前記複数のメディア・フロー識別子は、セッション記述におけるフローの順序を参照し、ゲートウェイ・ノードが、サービスに基づく個別ポリシー判断に応じて前記 1 つ以上のメディア・フローを許可する、コンピュータ読み取り可能媒体。

【請求項 1 3】

請求項 1 1 記載のコンピュータ読み取り可能媒体において、前記方法は、更に、第 2 メディア許可トークンを受信するステップと、前記第 2 メディア許可トークンを含むコンテキスト変更要求を送信し、前記 1 つ以上のメディア・フローの許可を変更するステップと、を含む、方法。

10

【請求項 1 4】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたネットワーク・ノードに、リソースを許可し配分する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

セッションの 1 つ以上のメディア・フローの各々を許可するためのメディア許可トークンを含むコンテキスト要求を受信するステップであって、前記メディア許可トークンと、複数のメディア・フロー識別子からのメディア・フロー識別子との組み合わせが、前記セッションの複数のメディア・フローの中からメディア・フローを一意に特定するのに十分である、ステップと、

前記メディア許可トークンが示すポリシー情報を要求するステップと、
から成るコンピュータ読み取り可能媒体。

20

【請求項 1 5】

請求項 1 4 記載のコンピュータ読み取り可能媒体において、前記複数のメディア・フロー識別子は、セッション記述におけるフローの順序を参照する、方法。

【請求項 1 6】

請求項 1 4 記載のコンピュータ読み取り可能媒体において、前記方法は、更に、サービスに基づく個別ポリシー判断に応じて、前記 1 つ以上のメディア・フローを許可するステップを含む、方法。

【請求項 1 7】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたユーザ機器に、セッションの 1 つ以上のパケット・メディア・フローについて許可および配分を要求する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

セッション・プロトコルの通知の間に、許可トークンおよびパケット・メディア・フロー情報を受信するステップであって、前記パケット・メディア・フロー情報が、ネットワーク・ノードおよび前記ユーザ機器にアクセス可能である、ステップと、

セッションの 1 つ以上のパケット・メディア・フローを許可するためにバインド情報を含む 1 つ以上のメッセージを送信するステップであって、前記バインド情報が前記許可トークンを含むことにより、前記 1 つ以上のメディア・フロー識別子の各々を、前記許可トークンに関して解釈し、前記セッションのパケット・メディア・フローを特定する、ステップと、

30

から成る、コンピュータ読み取り可能媒体。

40

【請求項 1 8】

請求項 1 7 記載のコンピュータ読み取り可能媒体において、前記ユーザ機器はセルラ・デバイスであり、前記ネットワーク・ノードは G G S N から成り、前記 1 つ以上のメッセージの各々は、P D P コンテキスト活性化または変更要求である、コンピュータ読み取り可能媒体。

【請求項 1 9】

請求項 1 7 記載のコンピュータ読み取り可能媒体において、前記 1 つ以上のパケット・メディア・フローは I P メディア・フローである、コンピュータ読み取り可能媒体。

【請求項 2 0】

50

請求項 17 記載のコンピュータ読み取り可能媒体において、前記 S D P 記述は、前記パケット・メディア・フロー情報を含み、前記 1 つ以上のパケット・メディア・フロー識別子は、前記 S D P 記述におけるメディアの順序を参照する、コンピュータ読み取り可能媒体。

【請求項 2 1】

請求項 17 記載のコンピュータ読み取り可能媒体において、前記セッション・プロトコルは S I P であり、P - C S C F の P C F が前記許可トークンを生成する、コンピュータ読み取り可能媒体。

【請求項 2 2】

請求項 17 記載のコンピュータ読み取り可能媒体において、前記ユーザ機器は、単一のメッセージを送信して、前記セッションの全てのパケット・メディア・フローについてのリソース許可および配分を要求する、コンピュータ読み取り可能媒体。 10

【請求項 2 3】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたネットワーク・ノードに、セッションの 1 つ以上のパケット・メディア・フローに対してリソースを許可および配分する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

セッション・プロトコルの通知の間に、許可トークンおよびパケット・メディア・フロー情報を送信するステップであって、前記パケット・メディア・フロー情報が、前記ネットワーク・ノードおよびユーザ機器にアクセス可能である、ステップと、 20

セッションの 1 つ以上のパケット・メディア・フローを許可するためにバインド情報を含む 1 つ以上のメッセージを処理するステップであって、前記バインド情報が前記許可トークンを含み、前記処理が、1 つ以上のパケット・メディア・フロー識別子の各々を前記許可トークンに関して解釈し、前記セッションのパケット・メディア・フローを特定する、ステップと、
から成るコンピュータ読み取り可能媒体。

【請求項 2 4】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記ユーザ機器はセルラ・デバイスであり、前記ネットワーク・ノードは G G S N から成り、前記 1 つ以上のパケット・メディア・フローは I P メディア・フローである、コンピュータ読み取り可能媒体。 30

【請求項 2 5】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、S D P 記述が前記パケット・メディア・フロー情報を含み、前記 1 つ以上のメディア・フロー識別子が前記 S D P 記述におけるメディアの順序を参照する、コンピュータ読み取り可能媒体。

【請求項 2 6】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記セッション・プロトコルは S I P であり、P - C S C F の P C F が前記許可トークンを生成する、コンピュータ読み取り可能媒体。

【請求項 2 7】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記ネットワーク・ノードは、前記セッションの全てのパケット・メディア・フローに対するリソースの許可および配分を要求する単一のメッセージを処理する、コンピュータ読み取り可能媒体。 40

【請求項 2 8】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記方法が、更に、前記許可トークンが示すポリシー情報を要求するステップを含む、コンピュータ読み取り可能媒体。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、パケット・メディア・フローのためのバインド機構(binding mechanism)に関 50

する。一実施形態では、このバインド機構は、許可トークンおよび1つ以上のフロー識別子を用いて、セッションの1つ以上のメディア・フローを特定し許可する。

【背景技術】

【0002】

本願は、2001年4月17日に出願した"Binding Information for IP Media Flows" (IPメディア・フローのためのバインド情報) と題する米国仮特許出願第60/284,358号の優先権を主張する。その内容は、ここで引用したことにより本願にも含まれることとする。

【0003】

最近の10年の間に、公衆が使用するセルラ・デバイスの数は爆発的に増大した。移動電話機は珍しくなくなり、ワイヤレス機能を備えたパーソナル・ディジタル・アシスタント(PDA)およびラップトップ・コンピュータも普及しつつある。セルラ・デバイスは、ワールド・ワイド・ウェブの閲覧、一方向および双方向オーディオおよびビデオ通信、インスタント・メッセージ送受信、ならびにその他の形式のマルチメディア情報の送受信にも用いられている。

【0004】

同じ期間に、インターネットは飛躍的に成長した。1990年初期には、インターネットは、電子メール、テキスト通信、またはファイル転送に用いられるのが通例であった。今日、インターネットは、これらの目的にも依然として使われているが、一方向オーディオおよびビデオ・ストリーミング(streaming)、双方向オーディオおよびビデオ通信、マルチメディア閲覧、およびメッセージ送受信にも用いられている。

【0005】

インターネットは、パケット交換型ネットワークの一例である。いかなる種類の情報がインターネット上で送られても、この情報はパケット単位で送信される。一般に、パケットは、1) パケットの発信元および宛先のアドレスを含むヘッダと、2) ひとまとまり(chunk)の情報を含むデータ・ペイロード部とを有する。パケットは、インターネット内でコンピュータからコンピュータに導かれ、発信元から宛先に供給される。インターネット・プロトコル[「IP」]とは、インターネットを通じてパケットを送信するための規則集である。別のパケット・データ・プロトコルが開発されるのと同様、種々のバージョンのIPも開発されている。

【0006】

インターネットは、電気通信ネットワークとして、様々な利点を提供する。これは地球全体に及び、機器の故障を補償する冗長性を含む。これは、種々の異なる形式のネットワークおよびユーザ機器と動作する。

【0007】

一方、インターネットの特性には、ある種の用途には適さないものもいくつかある。従来より、インターネットを通じたパケットの配信は、ベスト・エフォート・モデルにしたがって行われてきた。ルーティング・コンピュータ(即ち、ルータ)は、可能な限り最良の状態でパケットをルーティングするが、トラフィック量が溢れることもある。このようなときに、パケットの配信は遅れる可能性があり、あるいはパケットが欠落する可能性もある。電子メールのような用途では、これは実際には問題にならない。何故なら、配信時間はさほど重要ではなく、パケットを再送信することができるからである。しかしながら、他の用途では、遅延や不連続の問題は一層深刻となる。音声電話(audio telephony)やテレビ会議では、通信に容認可能な遅延量には限界がある。オーディオおよびビデオ・ストリーミングの限界はさほど厳しくないが、遅延や不連続の悪影響を受ける可能性はある。インターネットのベスト・エフォート・モデルは、より高いサービス品質[「QoS」]要件を有するオーディオ、ビデオ、およびその他のIPマルチメディア・アプリケーションの開発を阻害する。加えて、インターネット・ユーザには、インターネットを通じてユーザがどれだけパケットを送信または受信したかには関係なく、均一のアクセス料金が課金される。したがって、電子メールのためにインターネットを用いる人には、IPマルチメ

ディア・アプリケーションのためにインターネットを用いる人と比較すると、不均衡に課金されていると考えられる。更に、一層高いQoSを求めて高額の料金を支払おうとしても、その選択肢はない。

【0008】

最近の開発には、QoS要求が高い用途には適さない特性に取り組みつつ、インターネットの優れた特徴をいかに利用するかという点に照準をあてたものがある。他にも、移動電気通信やパケット交換ネットワーク双方を通じて通信するデバイスについて、移動電気通信ネットワークにおけるQoSおよび端末間のQoS(end-to-end QoS)に照準を当てた開発もある。

1. セッションの開始および記述プロトコル

10

セッション開始プロトコル[「SIP」]は、一人以上の参加者とのセッションを作成し、修正し、終了させるための規則集である。これらのセッションは、インターネット・マルチメディア会議、インターネット通話、およびマルチメディア配給(distribution)を含む。SIPは、主にセッションに関する情報を伝達するために用いられ、パケットのルーティングというようなことを制御する下位プロトコルの上で動作する。

【0009】

SIPメッセージは、セッション記述を、例えば、セッション記述プロトコル[「SDP」]にしたがって搬送することができ、これによって参加者はセッションのためのメディア・フローについて同意することができる。SDP記述は、セッション・レベルの記述(セッションおよびメディア・ストリームに適用される詳細を含む)、および0以上のマルチ・レベル記述(単一のメディア・ストリームに適用される詳細を含む)を含む。セッション・レベル記述は、セッション名(SDP記述において「s=」で始まるラインによって識別する)のような情報を含み、更に接続情報[「c=」]、帯域幅情報[「b=」]、およびその他の情報も含むことができる。メディア・レベル記述[「m=」]は、メディア種別(例えば、ビデオ、オーディオ)、トランスポート・プロトコル、およびフォーマット(例えば、MPEGビデオ)のような情報を含む。また、メディア・レベル記述は、接続情報、帯域幅情報、およびその他の情報も含むことができる。

20

【0010】

SIPは、ユーザの現在位置に対する要求を仲介(proxy)し、再送出することによって、ユーザの移動性に対応する。例えば、ユーザは、SIPプロキシを用いて彼の現在位置を登録することができ、プロキシは、SIP通知については、ユーザの仲介者として作用する。

30

【0011】

SIPは、ユーザ・エージェント[「UA」]およびSIPプロキシを用いて、呼の許可に対応するように拡張されている。UA(例えば、ユーザのセルラ・デバイス)は、信用できないと見なされる。UAが開始した呼では、SIPプロキシがUAへからのメディア・データを許可する。SIPプロキシは、メディア許可トークンをUAに供給する。UAがメディア・データを他の終点(end point)と交換する準備ができたときに、UAは、そのSIPプロキシから受信したメディア許可トークンを用いて、帯域幅を要求する。

【0012】

40

SIPおよびSDPに関するこれ以上の情報については、Internet Engineering Task Force(インターネット・エンジニアリング・タスク・フォース)[「IETF」]から発行されているRequest for Comment(コメントの要求)[「RFC」]2543およびRFC2327を参照のこと。前述のSIPの拡張については、"SIP Extensions for Media Authorization"(メディア許可のためのSIPの拡張)第1版と題するIETF Internet Draft(IETFインターネット草稿)を参照のこと。

II. 次世代インターネット・アーキテクチャ

インターネット上におけるQoSについての懸念に取り組むために、インターネットのこれまでのベスト・エフォート・モデルを変化させる様々なアーキテクチャが研究されている。これら次世代アーキテクチャには、Integrated Services in the Internet Architec

50

ture (インターネット・アーキテクチャにおける統合サービス) [「IntServ」] およびArchitecture for Differentiated Services (差別化サービスのためのアーキテクチャ) [「DiffServ」] が含まれる。

【0013】

IntServは、インターネットの従来からのベスト・エフォート・モデルに1組の拡張を規定する。IntServアーキテクチャでは、設定機構を用いて情報をルータに伝送し、要求されたサービスをルータが、そのサービスを要求したフローに提供できるようにしている。Resource Reservation Protocol (リソース予約プロトコル) [「RSVP」] は、設定機構の1つである。ホストは、RSVPを用いて、個々のデータ・フローに対するネットワークからの特定のQoSを要求する。ネットワークは、これに応じて、要求を認めるかまたは拒絶する。要求が認められると、該当するルータがQoSを提供するように構成される。IntServおよびRSVPに関する追加の情報については、RFC 1633、RFC 2205、および関連する仕様書を参照のこと。

【0014】

DiffServアーキテクチャでは、パケットは、多数の集約フロー、即ち、「クラス」の1つに分類される。パケット・ヘッダは、パケットのクラスを示すDiffServコードポイントを含む。DiffServネットワークの縁部にあるネットワーク・ノード (即ち、DiffServエッジ・ノード) は、適切なDSCPをパケット・ヘッダ内に置くことができる。DSCPに基づいて、DiffServルータは、DiffServネットワークにおける次のホップのために、異なるパケット転送処理をパケットに適用する。DiffServに関する追加の情報については、RFC 2474、RFC 2475、および関連する仕様書を参照のこと。

【0015】

インターネット使用料金に関する懸念に取り組むために、様々な許可および課金アーキテクチャが開発されている。アーキテクチャが異なると、課金はインターネットの使用 (例えば、トラフィックおよび/または接続時間)、移動電気通信ネットワークの使用、セッション、またはメディア・フローによって行われる。様々な用途において、セッションおよびフローに基づく課金は、簡略性という利点をエンド・ユーザに提供し、異なるネットワークに対する価格一括契約(pricing package)に柔軟性を提供する。追加の情報については、IETFおよび3rd Generation Partnership Project [「3GPP」] による関連仕様書を参照のこと。

III. 端末間QoS

インターネット上において2つのセルラ・デバイス間で情報が流れる場合、端末間QoSは、インターネットおよびセルラ・デバイス間のインターネットのQoSおよび移動電気通信ネットワーク (例えば、Global System for Mobile Communication (汎ヨーロッパ・デジタル移動通信システム) [「GSM」] またはUniversal Mobile Telecommunications System (万国移動電気通信システム) [「UMTS」] ネットワーク) のQoSに左右される可能性がある。

【0016】

3GPPは、移動電気通信ネットワークQoSおよび端末間QoSに関する数多くの仕様書を編成している。3rd Generation Technical Specification (第3世代技術仕様書) [「3GTS」] 23.060 v3.6.0は、移動電気通信ネットワーク上での、IPのようなPacket Data Protocol (パケット・データ・プロトコル) [「PDP」] を用いるパケット・サービスについて記載している。3GTS 23.107 v4.0.0は、UMTSネットワークに対するQoSフレームワークを記述している。3GTS 23.207 v1.2.0は、端末間QoSのフレームワークについて記載しており、異なるネットワーク間でQoS要件をどのようにマップする(map)かについて取り組んでいる。

A. ベアラ・サービス

一般に、ネットワーク上において所要のQoSを実現するためには、規定の特性および機能性を有するベアラ・サービス [「BS」]、[「ベアラ」] または [「サービス」] を、ネット

ワーク上においてサービスの提供元から宛先まで設定する。ベアラ・サービスは、契約したQoSの提供、例えば、制御シグナリング、ユーザ・プレーン・トランスポート、およびQoS管理機能性を可能にする態様を含む。図1は、従来技術による、ベアラ・サービス層状アーキテクチャ(100)を示す。特定のレイヤ上におけるベアラ・サービスは、下位のベアラが提供するサービスを用いて、上位のレイヤにサービスを提供する。他のアーキテクチャでは、図1に示すサービスの内1つ以上が欠けていたり、異なるサービス構成を用いたり、または異なるサービスを用いる場合がある。図1およびその中で照会しているサービスおよび構成要素に関する追加の情報については、3GTS23.207v1.2.0、3GTS23.107v4.0.0、および関連する仕様書を参照のこと。

B. ネットワーク・アーキテクチャの例

図2は、従来技術によるネットワーク・アーキテクチャ(200)の簡略化した例を示す。他のネットワーク・アーキテクチャも可能である。アーキテクチャ(200)は、一般的なパケット無線サービス[「GPRS」]、およびバックボーンIPネットワーク(240)(例えば、インターネット)を用いたUMTSネットワークを含む。

【0017】

図2では、ローカル・ユーザ機器[「UE」](210)は、例えば、携帯電話機のようなセルラ・デバイス、またはワイヤレス伝送機能を有するコンピュータである。サービスを提供するGPRS対応ノード[「SGSN」](220)およびゲートウェイGPRS対応ノード[「GGSN」](230)は、移動電気通信ネットワーク用GPRSに対応する機能性を備えており、同一または異なるネットワーク・ノード内に位置することができる。SGSN(220)は、例えば、ワイヤレス・チャネルによって、基地局と通信し、一方基地局は、無線伝送によって、UE(210)と通信する。GGSN(230)は、UMTSネットワークおよびバックボーンIPネットワーク(240)間でパケットをルーティングする(例えば、DiffServ Edge、IntServ/RSVPシグナリング、またはその他の機能を提供する)。

【0018】

IPベアラ・レイヤ(270)は、IPベアラ・サービス(272)を含み、UMTSネットワークおよびバックボーンIPネットワーク(240)にわたって、契約したQoSをUE(210)からリモート・ホスト(260)に提供する。アクセス・ベアラ・レイヤ(280)は、IPベアラ・レイヤ(270)の下位にあたるベアラ・サービスを含み、例えば、契約したQoSをUE(210)とGGSN(230)との間で提供するUMTSベアラ・サービスがある。図2は、リモート・アクセス・ポイント(250)や、バックボーンIPネットワーク(240)とリモート・ホスト(260)との間のアクセス・ベアラ・サービスの詳細を省いて抽象化している。リモート・ホスト(260)は、UE(210)側と同一であることも、異なることも可能である。

【0019】

UE(210)は、1つ以上のPDP(例えば、IP)アドレスを有し、これらは静的または動的に割り当てることができる。PDPコンテキスト・ベアラ(例えば、UMTSネットワークUEのGPRS)を通じて1つ以上のPDPコンテキストを設定する。例えば、PDPコンテキスト活性化要求の場合、UE(210)は指定したQoSのパケット・サービスを、PDPアドレスに対して、アクセス・ポイント名[「APN」]から要求する。APNは、外部パケット・データ・ネットワークおよび/またはサービスを参照し、要求をGGSNにマップする際に用いることができる。要求QoSは、QoSプロファイルによって指定することができる。

【0020】

QoSプロファイルとは、UMTSネットワークのようなネットワークのサービスを指定する1組の属性である。3GTS23.107V4.0.0は、4つの異なるUMTS QoSトラフィック・クラスについて記載しており、これらは主にトラフィックの遅延に対する感度が異なる。トラフィック・クラスに加えて、ベアラのユーザは、ネットワークが提供するサービスに対して他の属性も指定することができ、最大ビットレート、保証ビ

10

20

30

40

50

ットレート、および転送遅延が含まれる。

【0021】

【表1】

クラス	意図する使用
会話	オーディオおよびビデオ・テレフォニのように遅延に非常に敏感なトラフィック
ストリーミング	オーディオおよびビデオ・テレフォニ程遅延に敏感ではない非会話トラフィック
対話	WWW閲覧やインスタント・メッセージのような対話型アプリケーション
背景	背景ファイルまたは電子メールのダウンロードのような、遅延に鈍感なトラフィック

10

表1：TS 23.107 v4.0.0におけるUMTS QoSトラフィック・クラス

【0022】

SGSN (220) およびGGSN (230) は、加入者のプロファイル、現在のリソース、またはその他の判断基準に応じて、要求QoSを変更することができる。UE (210) は、PDPコンテキスト・ベアラを通じて、同じまたは異なるQoSで追加のPDP 20
コンテキストを要求することができる。また、UE (210) は、既存のコンテキストの所要の属性も修正することができる（例えば、PDPコンテキスト修正要求によって）。状況によっては、GGSNまたはその他のネットワーク・エンティティがコンテキストの活性化または修正を行うことができる。

【0023】

図2に関する追加の情報、その中で照会されているサービスおよび構成要素、その他のネットワーク・アーキテクチャ、PDP、QoSプロファイル、ならびにUMTSネットワークに対するQoSについては、3GTS 23.207 v1.2.0、3GTS 23.107 v4.0.0、3GTS 23.060 v3.6.0、および関連する仕様書を参照のこと。 30

C. ポリシーの施行およびQoS相互作用

図3は、従来技術による端末間IP QoSのためのQoS管理機能を有するフレームワーク (300) を示す。高レベルでは、図3は、UE (310)、セルラ基地局のネットワークのようなUTRAN (320)、SGSNのようなCN EDGE (330)、GGSNのようなゲートウェイ (340)、プロキシ呼セッション制御機能 [「P-CSCF」] (350)、および外部ネットワーク (36) を示す。簡略化のために、図3は、下位のベアラ・サービス機能を示していない。

【0024】

図3では、ゲートウェイ (340) は、IP BSマネージャ (342)、変換 (346) 機能、およびUMTS BSマネージャ (348) を含む。IP BSマネージャ (342) は、DiffServ Edge、RSVP/IntServシグナリング、ポリシー制御、またはサービス同意機能のような機構を用いて、外部ネットワーク (360) との相互作用を管理する。IP BSマネージャ (342) は、変換 (346) 機能を通じて、UMTS BSマネージャ (348) と通信する。変換 (346) 機能は、UMTSベアラ・サービスの機構およびパラメータ（例えば、QoSパラメータ）とIPベアラ・サービスのそれらとの間の相互作用を用意する (provide)。他のフレームワークも可能であり、例えば、UE (310) におけるIP BSマネージャおよび変換機能を含むもの、またはネットワーク間の相互作用のためのその他の機構を用いるものがある。 40

【0025】

フレームワーク (300) は、ポリシーに基づく承認 (admission) 制御に用いることがで 50

き、その場合、ポリシー制御機能〔「PCF」〕(353)が、ポリシー情報および規則を用いて、ネットワークに基づくIPポリシーに関する決定を行う。ポリシー情報要素は、例えば、アドレスや、セッションのIPフローに対して許可されたQoSを含む。PCF(353)は、ポリシー情報を、ゲートウェイ(34)内のIPBSマネージャ(342)に、インターフェースを通じて伝達する。IPマルチメディアおよびその他のサービスに対して、サービスに基づく個別ポリシー〔「SBLP」〕判断をペアラに適用することができる。SBLP判断は、UE(310)、ゲートウェイ(340)、およびP-CSCF(350)間の交流(interaction)を伴う。

【0026】

PCF(353)に加えて、P-CSCF(350)は、ローカルSIPプロキシ(351)を含み、SIPシグナリング、およびセッションのSDP記述の取得に用いる。P-CSCF(350)およびPCF(353)にはいくつかの役割があり、SDP記述に記述されているセッションに対してQoSリソースを許可することを含む。P-CSCF(350)/PCF(353)は、SIPセッションに対して許可トークンを生成し、許可トークンをUE(310)にSIPメッセージによって送ることができる。例えば、許可トークンは、メディア許可のためのSIP拡張に関するIETF仕様書に準拠する。

【0027】

UE(310)は、リソース予約要求を行い、ゲートウェイ(340)はこれをPCF(353)からの許可と照合する。例えば、UE(310)は、PDPコンテキスト活性化または修正要求内に、UMTS QoSパラメータと共に、許可トークンを含む。次いで、許可トークンは、要求をPCF(353)からの許可と相関付けるために用いることができる。

【0028】

ゲートウェイ(340)は、IPポリシー施行地点であり、いくつかの役割を有する。これは、IPパケットの1つまたは複数のQoSフローに対するアクセスを制御する。ポリシー情報は、PCF(353)によってゲートウェイ(340)に「押し出される」(push)か、またはゲートウェイ(340)によってPCF(353)から要求されるかのいずれかである。また、ゲートウェイ(340)は、フロー/ゲーティング制御機能性も備えており、あるフローのIPパケットが許可を超過した場合処置を講ずる。

【0029】

図3ならびにその中で照会したサービスおよび構成要素に関する追加の情報については、3GTS23.207v1.2.0、および関連する仕様を参照のこと。

【非特許文献1】

Request for Comment〔「RFC」〕2543

【非特許文献2】

RFC2327

【非特許文献3】

"SIP Extensions for Media Authorization"第1版

【非特許文献4】

RFC1633

【非特許文献5】

RFC2205

【非特許文献6】

RFC2474

【非特許文献7】

RFC2475

【非特許文献8】

3GTS23.207v1.2.0

【非特許文献9】

3GTS23.107v4.0.0

30

40

50

【非特許文献10】

3 G T S 2 3 . 0 6 0 v 3 . 6 . 0

【発明の開示】

【発明が解決しようとする課題】

【0030】

一般に、フロー毎の許可では、セッション毎の許可よりも、許可、QoS管理、および課金に関して、一層精細な制御が行われる。しかしながら、SIPシグナリング中に生成される許可トークンは、セッションの多数の異なるフローを個々に特定し許可を与えるには適していない。

【0031】

本発明は、パケット・メディア・フローのためのバインド機構に関する。バインド機構は、許可トークンおよびパケット・メディア・フロー識別子を用いて、セッションのパケット・メディア・フローを特定し許可を与える。これによって、セッション毎の許可トークンを用いつつ、セッションの個々のパケット・メディア・フローに基づくリソースの許可および配分を可能にするという利点を得られる。バインド機構は種々の態様を含む。

【課題を解決するための手段】

【0032】

第1の形態によれば、装置は、セッションの1つ以上のパケット・メディア・フローを許可するためにバインド情報を含む1つ以上のメッセージを送信する。バインド情報は、許可トークンを含み、パケット・メディア・フロー識別子と組み合わせると、セッションのパケット・メディア・フローを特定するのに十分となる。例えば、UEが、バインド情報を含む1つ以上のPDPコンテキスト要求を送信する。バインド情報は、SIPメディア許可トークンと、1つ以上のIPメディア・フロー識別子とを含む。

【0033】

第2の形態によれば、ネットワーク・ノードが、セッションの1つ以上のパケット・メディア・フローを許可するために、バインド情報を処理する。バインド情報は、許可トークンを含む。ネットワーク・ノードは、許可トークンに関して、1つ以上のパケット・メディア・フロー識別子の各々を解釈し、セッションのパケット・メディア・フローを特定する。例えば、バインド情報は、SIPメディア許可トークンと、1つ以上のIPメディア・フロー識別子とを含む。

【0034】

本発明の更に別の特徴および利点は、添付図面を参照しながら進める、以下の実施形態の詳細な説明から明白となる。

【発明を実施するための最良の形態】

【0035】

記載する本発明の実施形態は、セッションの1つ以上のIPメディア・フローに対して要求されたQoSを許可するバインド機構を対象とする。UEからGGSNに送信されるバインド情報は、SIPメディア許可トークンを含む。GGSNは、1つ以上のIPメディア・フロー識別子を、SIPメディア許可トークンに関して解釈し、セッションの1つ以上のIPメディア・フローを特定する。伝送帯域幅、計算上の複雑さ、およびシグナリングの複雑さに関して、セッション毎の許可トークンの仕様は、セッションのIPメディア・フロー毎に異なる許可トークンを用いるよりも一層効率的である。同時に、セッション毎の許可トークンと共に多数のIPメディア・フロー識別子を用いることによって、セッションの個々のIPメディア・フローに基づく、リソース許可および配分のための簡単な機構が設けられる。

【0036】

記載する実施形態では、バインド機構は、いくつかの技法およびシステムを含む。これらの技法およびシステムは、ここでは、単一の統合化フレームワークの一部として説明するのが通例であるが、これらの技法およびシステムは、別個に、潜在的には他の技法およびシステムと組み合わせて適用することができる。

【0037】

記載する実施形態では、バインド機構は、種々の技術的仕様書に準拠したシステムの一部であり、仕様書には、最も特筆すべきものとして3GTS23.207が含まれるが、3GTS23.107、3GTS23.060、および"SIP Extensions for Media Authorization" (メディア許可のためのSIP拡張)と題するIETFインターネット草稿も含まれる。代替の実施形態では、バインド機構は、他のシステムにおいて、および／または他のプロトコルと動作する。

【0038】

表2は、本願において用いられる頭字語および略語の一部を纏めたものである。

【0039】

【表2】

短縮形	用語全体
3GTS	第3世代技術仕様書
3GPP	第3世代パートナーシップ・プロジェクト
APN	アクセス・ポイント名
BS	ベアラ・サービス
DiffServ	差別化サービス用アーキテクチャ
DSCP	DiffServコードポイント
GGSN	ゲートウェイGPRS対応ノード
GPRS	総合パケット無線サービス
GSM	汎ヨーロッパ・デジタル移動通信システム
IETF	インターネット・エンジニアリング・タスク・フォース
IntServ	インターネット・アーキテクチャにおける統合サービス
IP	インターネット・プロトコル
PCSCF	プロキシ呼セッション制御機能
PCF	ポリシー制御機能
PDA	パーソナル・デジタル・アシスタント
PDP	パケット・データ・プロトコル
QoS	サービス品質
RFC	コメント要求
RSVP	リソース予約プロトコル
SBLP	サービス基準個別ポリシー
SDP	セッション記述プロトコル
SGSN	サービス供給GPRS対応ノード
SIP	セッション開始プロトコル
UA	ユーザ・エージェント
UE	ユーザ機器
UMTS	万国移動電気通信システム
UTRAN	UMTS地上無線アクセスネットワーク

表2：頭字語および略語

【0040】

1. 計算機環境

図4は、ここに記載する実施形態を実現可能な、相応しい計算機環境(400)の一般化した例を示す。計算機環境(400)は、本発明の使用または機能性の範囲に関してはいづれの限定をも示唆することを意図していない。本発明は、セルラ・デバイスまたはその他のユーザ機器、あるいはGGSNまたはその他のネットワーク・ノードというような、多様な汎用または特殊目的計算機環境において実現することができる。

【0041】

図4を参照すると、計算機環境(400)は、少なくとも1つの処理ユニット(410)

とメモリ（４２０）とを含む。図４では、この最も基本的な構成（４３０）は、破線の中に含まれている。処理ユニット（４１０）は、コンピュータ実行可能命令を実行し、実プロセッサまたは仮想プロセッサでもよい。マルチ処理システムでは、多数の処理ユニットがコンピュータ実行可能命令を実行して処理能力を高める。メモリ（４２０）は、揮発性メモリ（例えば、レジスタ、キャッシュ、RAM）、不揮発性メモリ（例えば、ROM、EEPROM、フラッシュ・メモリなど）、またはこれら２つの何らかの組み合わせとすればよい。メモリ（４２０）は、許可トークンおよび１つ以上のフロー識別子によってバインド機構を実現するソフトウェア（４８０）を格納する。

【００４２】

計算機環境は、追加の構成を有することもできる。例えば、計算機環境（４００）は、ストレージ（４４０）、１つ以上の入力デバイス（４５０）、１つ以上の出力デバイス（２６０）、および１つ以上の通信接続部（４７０）を含む。バス、コントローラ、またはネットワークのような相互接続機構（図示せず）が、計算機環境（４００）の構成要素を相互接続する。通例では、オペレーティング・システム・ソフトウェア（図示せず）が、計算機環境（４００）内で実行するその他の動作環境を設け、計算機環境（４００）の構成要素のアクティビティを調整する。

【００４３】

ストレージ（４４０）は、着脱可能または固定のいずれでもよく、磁気ディスク、磁気テープまたはカセット、CD-ROM、CD-RW、DVD、あるいは情報を格納するために使用でき、計算機環境（４００）内部でアクセス可能な媒体であれば他のいずれでもよい。ストレージ（４４０）は、許可トークンおよび１つ以上のフロー識別子によってバインド機構を実現するソフトウェア（４８０）のコンピュータ実行可能命令を格納することができる。

【００４４】

１つ以上の入力デバイス（４５０）は、数値キーパッドのような接触式入力デバイス、キーボード、マウス、ペン、トラックボール、音声入力デバイス、走査デバイス、または計算機環境（４００）に入力を供給するその他のデバイスとすることができる。１つ以上の出力デバイス（４６０）は、ディスプレイ、プリンタ、スピーカ、CD-ライター、または計算機環境（４００）からの出力を供給するその他のデバイスとすることができる。

【００４５】

１つ以上の通信接続部（４７０）は、通信媒体を通じて別の計算機エンティティへの通信を可能にする。通信媒体は、コンピュータ実行可能命令、オーディオまたはビデオ情報、あるいは変調データ信号におけるその他データというような情報を伝達する。変調データ信号とは、その特徴の１つ以上が、当該信号の中に情報をエンコードするように設定または変化されている信号のことを言う。限定ではなく、一例として、通信媒体は、無線周波数と共に用いられる有線またはワイヤレス媒体、電氣的、光学的、赤外線、音響、またはその他のキャリアを含む。

【００４６】

本発明の説明は、一般的なコンピュータ読み取り可能媒体との関連で行うことができる。コンピュータ読み取り可能媒体は、計算機環境内部においてアクセス可能で、入手可能なあらゆる媒体のことである。限定ではなく、一例として、計算機環境（４００）では、コンピュータ読み取り可能媒体は、メモリ（４２０）、ストレージ（４４０）、通信媒体、およびこれらのいずれの組み合わせをも含む。

【００４７】

本発明の説明は、目的の実プロセッサまたは仮想プロセッサ上の計算機環境において実行するプログラム・モジュールに含まれるような、一般的なコンピュータ実行可能命令との関連で行うことができる。一般に、プログラム・モジュールは、ルーチン、プログラム、ライブラリ、オブジェクト、クラス、コンポーネント、データ構造等を含み、個々のタスクを実行するか、あるいは個々の抽象的データ形式を実現する。プログラム・モジュールの機能性は、必要に応じて、種々の実施形態においてプログラム・モジュール間で組み合

わせたり、あるいは分割することもできる。プログラム・モジュールのコンピュータ実行可能命令は、ローカルまたは分散計算機環境内でも実行可能である。

【0048】

念のため断っておくが、詳細な説明では、「要求」、「発生する」、および「変更する」といような用語を用いて、計算機環境におけるコンピュータの動作を説明する。これらの用語は、コンピュータが実行する動作についての上位抽象概念であり、人が行う活動と混同してはならない。これらの用語に対応する実際のコンピュータの動作は、実現例に応じて異なる。

I I. バインド機構

ここに記載するバインド機構は、GGSNにおいてPDPコンテキスト・ベアラをポリシー情報と関連付け、SBLPの施行およびQoS相互作用を支援するものである。GGSNにおけるポリシー情報は、IPメディア・フローに基づく。バインド機構は、PDPコンテキスト・ベアラと関連がある1つ以上のIPメディア・フローを特定し、適用するポリシー情報を選択する際に、この特定情報を用いる。 10

【0049】

バインド機構には、UEが提供するバインド情報（例えば、許可トークンおよび1つ以上のフロー識別子）で、PDPコンテキスト上で搬送される1つ以上のIPメディア・フローを特定するには十分である。バインド機構は、SIPシグナリングおよびPDPコンテキスト活性化/変更メッセージに1つの許可トークンを保持しつつ、IPメディア・フローに基づいてリソースの許可および配分を可能にする。これによって、セッション毎に1つの許可トークンを用いればよいという利点、およびフロー毎にリソースの許可および配分ができるという利点が得られる。 20

【0050】

ポリシー情報としては、例えば、P-CSCF/PCFは、セッションのSDP記述を用いて、当該セッションの許可を判断し、ポリシー情報は、IPリソースに対する制約、IPパケット・フロー、および（潜在的に）IP宛先を含む。許可されたセッションは、1つ以上のフロー許可を含むことができ、各フロー許可は、フローに対するIPフロー5タプル（即ち、ソース・アドレスおよびポート、宛先アドレスおよびポート、プロトコル）、フローに対して許可されたりソースの仕様、およびフローのホップ挙動毎に割り当てられるDiffServを識別するDSCPを保持する。 30

【0051】

IPポリシー施行は、IPメディア・フローに基づくが、一方UMTSベアラは、UEからGGSNへのPDPコンテキストに基づく。PDPコンテキストが活性化または変更され、SBLPが有効である場合、GGSNは、IPメディア・フローに伴うポリシー情報を用いて、ベアラを許可する。UEは、IPメディア・フローのPDPコンテキストへのマッピングを制御し、UEは、GGSNにバインド情報を提供して、PDPコンテキスト活性化/変更要求メッセージのためにポリシー情報を正しく特定できるようにする。そうでないと、GGSNは、ベアラを許可するために必要なポリシー情報を特定する十分な情報を有することができない。

【0052】

これまで、IETF SIPワーキング・グループは、SDP記述におけるIPメディア毎の許可トークンを用いて、UEがGGSNにバインド情報として与えることができるのはどれか検討していた。アーキテクチャに関しては正しいが、この手法では、SDPを変更し、PCF、GGSN、およびUE間でより多くの情報を送る必要がある。 40

【0053】

対照的に、ここに記載するバインド機構では、IPメディア・フローを特定するには、SDP記述におけるこれらの順序を用いる。例えば、最初のメディア・フロー（SDP記述において「m=」で始まるラインによって特定する）はフロー1であり、2番目のフローはフロー2等とする。P-CSCF/PCFおよびUE双方ともSDP記述を有するので、これらは一貫した方法でフローを特定する。P-CSCF/PCFからの許可情報、お 50

よびUEからのバインド情報は、双方とも1つ以上のメディア・フローを特定することができる。

【0054】

図5および図6は、許可トークンおよび1つ以上のIPメディア・フロー識別子を用いたバインド機構の技法(500、600)を示す。図5および図6は、概略的に、バインド機構のタイミングを示し、実際のタイミングは基礎をなすプロトコル(例えば、SIPおよびPDP)、ネットワーク等に左右される。

【0055】

図5および図6を参照すると、SIPシグナリングの間、P-CSCF/PCFは許可トークンおよびSDP記述をUEに送信する(610)。UEは、許可トークンおよびSDP記述を受信する(510)。

【0056】

次に、UEはPDPコンテキスト要求を送信する(520)。PDPコンテキストを活性化/変更する場合、UEは許可トークンをバインド情報として要求に含ませる。メディア・フローを正しくPDPコンテキストにマップするためには、UEは、SDP記述にしたがって、1つ以上のフロー識別子も含めなければならない。(許可トークンは、SIPシグナリングの間にP-CSCF/PCFによってUEに送られ(610)、フロー識別子は、SDP内の一連のメディア・フローにしたがってUEによって導き出されている。)フロー識別子は、少数のビットだけで済むので、エアリンクの挙動に及ぼす影響は最少である。即ち、バインド情報は、PDPコンテキスト活性化/変更メッセージに含まれ、PDPコンテキスト・ベアラをポリシー情報と関連付ける。PDP構成オプション・パラメータ(PDPコンテキスト活性化/変更要求において通知されるオプションのパラメータ)が、この目的のために用いられる。あるいは、PDPコンテキストのトラフィック・フロー・テンプレート・パラメータのような、別のパラメータを用いる。

【0057】

許可トークンは、APNに関連するPDPコンテキスト全体にわたって一意であり、メディア許可のSIP拡張に関するIETF仕様に準拠する。

フロー識別子は、SIPセッションに伴うIPメディア・フローを特定する。前述のように、フロー識別子は、SDP記述におけるメディア・フローの順序に基づくことができる。この場合、フロー識別子を許可トークンと組み合わせれば、IPメディア・フローを一意に特定するには十分である。何故なら、フロー識別子は、許可トークンに関して解釈されるからである。

【0058】

QoSおよびポリシー情報をPCFから「引き出す」ためには、GGSNが、用いるPCFのアドレスも許可トークンによって決定できるようにするとよい。

GGSNは、PDPコンテキスト要求を受信し(620)、PDPコンテキスト要求を処理する。例えば、GGSNは、含まれるバインド情報を用いて、PDPコンテキスト・ベアラと関連がある1つ以上のIPメディア・フローを特定し(630)、PCFにポリシー情報を問い合わせ(640)、バインド情報によって特定された1つ以上のIPメディア・フローに適用し、1つ以上のIPメディア・フローと関連がある、受信したポリシー情報をを用いて、ポリシー情報に関して適切であれば、ベアラを許可する(650)。

【0059】

SIPセッション変更の結果、メディア・フローの追加または削除のような変化をSDP記述に生ずる可能性がある。(例えば、一実現例では、メディア・フローを削除すると、対応する「m」ラインはなおもSDP記述の中にあるが、「m=0」に設定される。対応して、この削除されたフローに対して許可されたQoSリソースもPCFにおいて0に設定される。新たなメディア・フローが追加されると、これは既存のSDP記述の終端に追加される。)P-CSCF/PCFは、SDP記述が変化した場合、新たな許可トークンを発行することができる。SIPセッション変更の結果として、PDPコンテキストに関連するリソースが増大した場合、UEは古い(または新しい)許可トークンおよびフロー

識別子と共に、PDPコンテキストの変更を送る。

【0060】

以上、記載した所要の実施形態を参照しながら、本発明の原理について説明し例示したが、記載した実施形態は、このような原理から逸脱することなく、その構成および詳細において変更が可能であることは認められよう。尚、ここに記載したプログラム、プロセス、または方法は、特に指示がない限り、いずれの特定の形式の計算機環境にも関係付けられ、限定されたりはしないことは言うまでもない。ここに記載した教示にしたがって、種々の形式の汎用計算機環境または特殊計算機環境を用い、それに応じた動作を行うこともできる。記載した実施形態において、ソフトウェアとして示した要素は、ハードウェアでも実現可能であり、その逆も可能である。

10

【0061】

本発明の原理は多くの実施形態にも適用可能であることに鑑み、特許請求の範囲およびその均等物の範囲および精神に該当し得るあらゆる実施形態を、本発明として主張する。

【図面の簡単な説明】

【0062】

【図1】図1は、従来技術によるベアラ・サービス層状アーキテクチャの図である。

【図2】図2は、従来技術によるネットワーク・アーキテクチャの簡略化した例の図である。

【図3】図3は、従来技術による端末間IP QoSのためのQoS管理機能を示す図である。

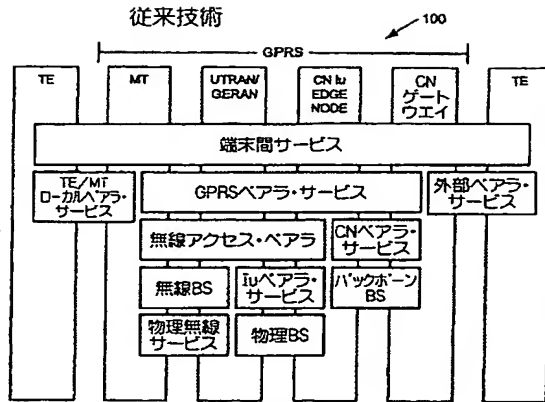
20

【図4】図4は、記載する実施形態を実現可能な、相応しい計算機環境のブロック図である。

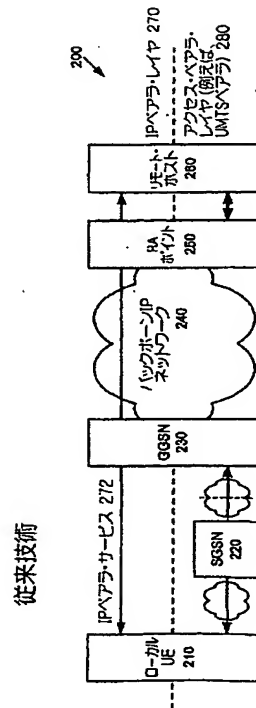
【図5】図5は、許可トークンおよび1つまたは複数のIPメディア・フロー識別子を用いたバインド機構のための技法のフロー・チャートである。

【図6】図5は、許可トークンおよび1つまたは複数のIPメディア・フロー識別子を用いたバインド機構のための技法のフロー・チャートである。

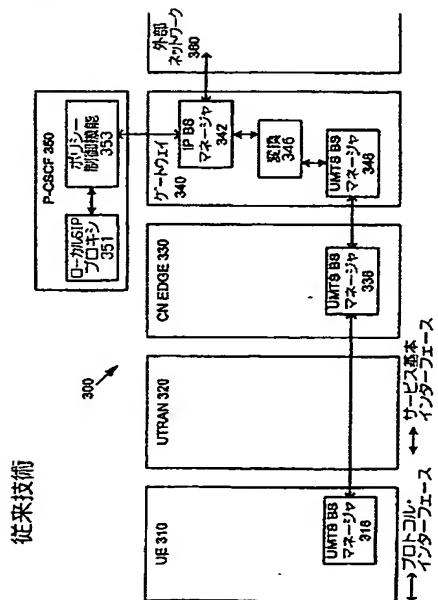
【図 1】



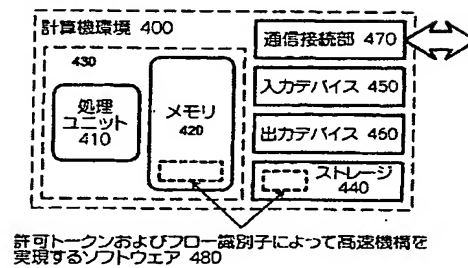
【図 2】



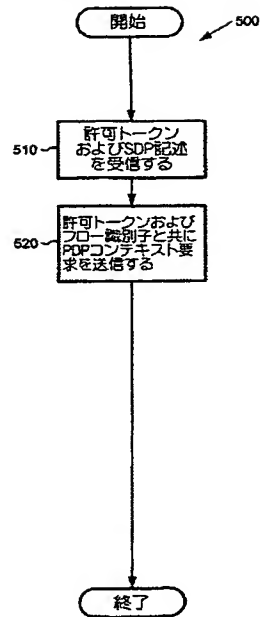
【図 3】



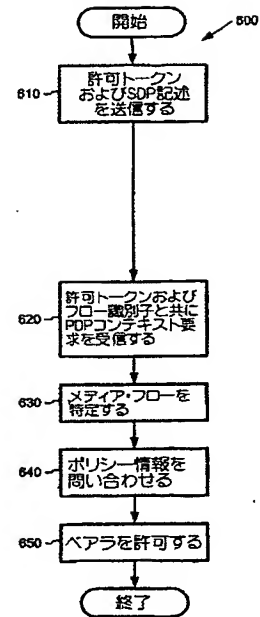
【図 4】



【図 5】



【図 6】



【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
24 October 2002 (24.10.2002)

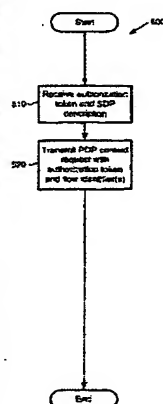
PCT

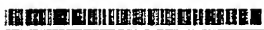
(10) International Publication Number
WO 02/085055 A2

- (51) International Patent Classification: H04Q 7/24 (US/US); 21433 St 33rd Place, Sammamish, WA 98075 (US).
- (71) International Application Number: PCT/US02/12181
- (74) Agent: RINEHART, Kyle, R. Klaydon Sparkman, LLP, One World Trade Center, Suite 1600, 121 SW Salmon Street, Portland, OR 97204 (US).
- (22) International Filing Date: 16 April 2002 (16.04.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/284,558 17 April 2001 (17.04.2001) US
104791/007 4 March 2002 (04.03.2002) US
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GR, GU, HK, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NZ, OM, PA, PE, PG, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, ST, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, HU, IE, IT, JP, NL, PT, SE, SI, SK, TR, UA, UK, US), OAPI patent (BF, BJ, GM, GN, GU, KE, ML, MR, NE, NG, SN, TD, TG).
- (72) Inventor: and
(73) Inventor/Applicant (for US only): SHLEH, Hugh, H.
- (54) Title: BINDING INFORMATION FOR IP MEDIA FLOWS
- (57) Abstract: A binding mechanism uses an authorization token and packet media flow identifier(s) to identify packet media flow(s) of a session for authorization. This provides the advantages of using a per-session authorization token while also allowing resource authorization and allocation on the basis of individual packet media flows of the session. The binding mechanism includes various aspects.



WO 02/085055 A2



WO 02/085055 A2 

GB, GR, IL, IE, LU, MC, NL, PL, SE, TR, UA, (w/acc)
(HU, BJ, CZ, DE, DK, EM, EA, EP, FR, GR, IT, JP, KR, NL, NO,
PT, SM, TR, TT).

Declaration under Rule 4.17
of annex (Rule 4.17(b)) for US only

Published:
— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette

WO 02/085053

PCT/US02/11181

1

BINDING INFORMATION FOR IP MEDIA FLOWS

RELATED APPLICATION INFORMATION

The present application claims the benefit of U.S. Provisional Patent Application Serial No. 60/284,358, entitled "Binding Information for IP Media Flows," filed April 17, 2001, the disclosure of which is incorporated by reference.

TECHNICAL FIELD

The present invention relates to a binding mechanism for packet media flows. In one embodiment, the binding mechanism uses an authorization token and one or more flow identifiers to identify one or more media flows of a session for authorization.

BACKGROUND

In the last ten years, the number of cellular devices used by the public has exploded. Mobile telephones are commonplace, and personal digital assistants ["PDAs"] and laptop computers with wireless capability are increasingly popular. Cellular devices are used for browsing the World Wide Web, one-way and two-way audio and video communication, instant messaging, and transmitting and receiving other types of multimedia information as well.

Over the same period, the Internet has grown tremendously. In the early 1990's, the Internet was typically used for email, text communication, or file transfer. Today, the Internet is still used for these purposes, but it is also used for one-way audio and video streaming, two-way audio and video communication, multimedia browsing, and messaging.

The Internet is an example of a packet-switched network. Whatever kind of information is sent over the Internet, the information is transmitted in packets. In general, a packet has 1) a header with addresses of the sender and destination for the packet and 2) a data payload portion with a chunk of the information. Packets are routed from computer to computer within the Internet to get from the sender to the destination. Internet Protocol ["IP"] is a set of rules for transmitting packets over the Internet. Various versions of IP have been developed, as have other packet data protocols.

WO 02/085055

PCT/US02/21811

2

The Internet offers several advantages as a telecommunications network. It spans the globe and includes redundancy to compensate for equipment failure. It operates with a variety of different types of networks and end user equipment.

On the other hand, several traits of the Internet make it unsuitable for certain applications. Conventionally, delivery of packets over the Internet happens according to a best effort model. A routing computer (i.e., router) routes packets as best it can, but sometimes gets overwhelmed with the amount of traffic. At such times, delivery of packets can be delayed or packets can get dropped. For applications such as email this is not really a problem, because delivery time is not critical and packets can be re-transmitted. For other applications, however, delay and discontinuity are more problematic. Audio telephony and videoconferencing have limits on the amount of delay that is acceptable for communication. Audio and video streaming have less stringent limits, but also can suffer from delay and discontinuity. The best effort model of the Internet hinders the development of audio, video, and other IP multimedia applications that have higher quality of service ["QoS"] requirements. In addition, Internet users are typically charged a flat access fee unrelated to how many packets the user transmits or receives over the Internet. People using the Internet for email can thus be charged disproportionately compared to people using the Internet for IP multimedia applications. Moreover, people who would pay more for higher QoS do not have that option.

Some recent developments have focused on how to take advantage of the good features of the Internet while addressing the traits that make it unsuitable for applications with higher QoS requirements. Other developments have focused on QoS in mobile telecommunications networks and end-to-end QoS for devices that communicate across both mobile telecommunications and packet-switched networks.

1. Session Initiation and Description Protocols

Session Initiation Protocol ["SIP"] is a set of rules for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls and multimedia distribution. SIP is mainly used for signaling information about sessions, and operates on top of lower-level protocols that control things such as routing of packets.

WO 02/085055

PCT/US02/1181

3

A SIP message can carry a session description, for example, according to Session Description Protocol ("SDP"), which allows participants to agree about the media flows for the session. A SDP description includes a session-level description (with details that apply to the session and the media streams) and zero or more media-level descriptions (with details that apply to a single media stream). The session-level description includes information like session name (identified by a line beginning with "s=" in the SDP description), and can also include connection information ("c="), bandwidth information ("b="), and other information. A media-level description ("m=") includes information such as media type (e.g., video, audio), transport protocol, and format (e.g., MPEG video). A media-level description can also include connection information, bandwidth information, and other information.

SIP supports user mobility by proxying and redirecting requests to the user's current location. For example, a user can register his current location with a SIP proxy, which acts as an intermediary for the user for SIP signalling.

SIP has been extended to support call authorization using user agents ("UAs") and SIP proxies. UAs (e.g., cellular devices of users) are considered untrusted. For a UA-initiated call, a SIP proxy authorizes media data to/from the UA. The SIP proxy supplies a media authorization token to the UA. When the UA is ready to exchange a media data with another endpoint, the UA requests bandwidth using the media authorization token it received from its SIP proxy.

For more information about SIP and SDP, see Request for Comment ("RFC") 2543 and RFC 2327 from the Internet Engineering Task Force ("IETF"). For the SIP extension described above, see the IETF Internet Draft entitled "SIP Extensions for Media Authorization," version 1.

11. Next Generation Internet Architectures

To address concerns with QoS over the Internet, various architectures have been researched which change the traditional best effort model of the Internet.

These next generation architectures include the Integrated Services in the Internet Architecture ("IntServ") and the Architecture for Differentiated Services ("DiffServ").

IntServ defines a set of extensions to the traditional best effort model of the Internet. In the IntServ architecture, a setup mechanism is used to convey information to routers so that the routers can provide requested services to flows that require the services. Resource Reservation Protocol ("RSVP") is one setup

WO 02/085055

PCT/US02/12189

4

mechanism. With RSVP, a host requests a specific QoS from the network for a particular data flow. The network responds by admitting or rejecting the request. For admitted requests, the appropriate routers are configured to provide the QoS. For additional information about IntServ and RSVP, see RFC 1633, RFC 2205, and related specifications.

In the DiffServ architecture, packets are classified into one of multiple aggregated flows or "classes." A packet header includes a DiffServ codepoint ["DSCP"] indicating the class of the packet. A network node at the edge of the DiffServ network (i.e., a DiffServ edge node) can place an appropriate DSCP in the packet header. Based on the DSCP, a DiffServ router can apply different packet forwarding treatment to the packet for the next hop in the DiffServ network. For additional information about DiffServ, see RFC 2474, RFC 2475, and related specifications.

To address concerns about charging for Internet usage, various authorization and charging architectures have been explored. Different architectures charge by Internet usage (e.g., traffic and/or connection time), mobile telecommunications network usage, session or media flow. In various applications, charging by session and flow offers the advantages of simplicity to the end user and flexibility in pricing packages for different networks. For additional information, see the relevant specifications by the IETF and the 3rd Generation Partnership Project ["3GPP"].

III. End-to-End QoS

When information flows over the Internet between two cellular devices, end-to-end QoS can depend on the Internet QoS as well as the QoS for the mobile telecommunications networks (e.g., Global System for Mobile Communication ["GSM"] or Universal Mobile Telecommunications System ["UMTS"] network) between the Internet and the cellular devices.

The 3GPP has organized numerous specifications relating to mobile telecommunications networks QoS and end-to-end QoS. 3rd Generation Technical Specification ["3G TS"] 23.060 v3.6.0 describes packet services that use a Packet Data Protocol ["PDP"] like IP over a mobile telecommunications network. 3G TS 23.107 v4.0.0 describes a QoS framework for UMTS networks. 3G TS 23.207 v1.2.0 describes a framework for end-to-end QoS and addresses how to map QoS requirements between different networks.

WO 02/08505A

PCT/US02/12181

5

A. Bearer Services

In general, to realize a certain QoS over a network, a bearer service ["BS," "bearer," or "service"] with defined characteristics and functionality is set up from the source to the destination of the service over the network. A bearer service includes aspects that enable the provision of a contracted QoS, for example, control signalling, user plane transport, and QoS management functionality. Figure 1 shows a bearer service layered architecture (100) according to the prior art. A bearer service on a specific layer uses services provided by the layers below and offers services to the layers above. Other architectures lack one or more of the services shown in Figure 1, use a different configuration of services, or use different services. For additional information about Figure 1 and the services and components referenced therein, see 3G TS 23.207 v1.2.0, 3G TS 23.107 v4.0.0, and related specifications.

B. Example Network Architecture

Figure 2 shows a simplified example of a network architecture (200) according to the prior art. Other network architectures are possible. The architecture (200) includes a UMTS network using a general packet radio service ["GPRS"] and a backbone IP network (240) (e.g., the Internet).

In Figure 2, the local user equipment ["UE"] (210) is, for example, a cellular device such as a mobile telephone or computer with wireless transmission capability. The serving GPRS support node ["SGSN"] (220) and the gateway GPRS support node ["GGSN"] (230) contain functionality to support GPRS for mobile telecommunications networks, and can be in the same or different network nodes. The SGSN (220) communicates, for example, by wireline channel with a base station that in turn communicates by radio transmission with the UE (210). The GGSN (230) routes packets (e.g., providing DiffServ Edge, IntServ/RSVP signalling, or other functions) between the UMTS network and the backbone IP network (240).

The IP Bearer Layer (270) includes an IP Bearer Service (272) for providing a contracted QoS from the UE (210) to the remote host (260), spanning the UMTS network and the backbone IP network (240). The Access Bearer Layer (280) includes bearer services underneath the IP Bearer Layer (270), for example, a UMTS Bearer Service for providing a contracted QoS between the UE (210) and

WO 02/085055

PCT/US02/12181

6

the GGSN (230). Figure 2 abstracts away the details of the remote access point (250) and access bearer service between the backbone IP network (240) and the remote host (260), which can mirror the UE (210) side or be different.

The UE (210) has one or more PDP (e.g., IP) addresses, which can be statically or dynamically assigned. One or more PDP contexts are set up across the PDP context bearer (e.g., the GPRS over the UMTS network). For example, with a PDP Context Activation request, the UE (210) requests a packet service with a specified QoS for a PDP address from a Access Point Name ("APN"). The APN refers to an external packet data network and/or a service, and can be used in mapping the request to a GGSN. The requested QoS can be specified with a QoS profile.

A QoS profile is a set of attributes specifying the service for a network such as a UMTS network. 3G TS 23.107 v4.0.0 describes four different UMTS QoS traffic classes, which differ mainly in how delay sensitive the traffic is. In addition to traffic class, a user of the bearer can specify other attributes for the service provided by the network, including maximum bitrate, guaranteed bitrate, and transfer delay.

Class	Intended Use
conversational	Very delay-sensitive traffic such as audio and video telephony.
streaming	Non-conversational traffic, which are less delay-sensitive than audio and video telephony.
interactive	Interactive applications like WWW browsing and instant messaging.
background	Delay-insensitive traffic such as background file or email downloading.

Table 1: UMTS QoS traffic classes in TS 23.107 v4.0.0

The SGSN (220) and the GGSN (230) can modify the requested QoS according to a subscriber profile, current resources, or other criteria. The UE (210) can request additional PDP contexts at the same or different QoS over the PDP context bearer. The UE (210) can also modify certain attributes of existing PDP contexts (e.g., with a PDP Context Modification request). In some circumstances, the GGSN or other network entities can activate or modify contexts.

For additional information about Figure 2, the service and components referenced therein, other network architectures, PDP, QoS profiles, and QoS for UMTS networks, see 3G TS 23.207 v1.2.0, 3G TS 23.107 v4.0.0, 3G TS 23.069 v3.6.0, and related specifications.

WO 02/085055

PCT/US02/2181

7

C. Policy Enforcement and QoS Inter-Working

Figure 3 shows a framework (300) with QoS management functions for end-to-end IP QoS according to the prior art. At a high level, Figure 3 shows UE (310), a UTRAN (320) such as a network of cellular base stations, a CN EDGE (330) such as a SGSN, a gateway (340) such as a GGSN, a proxy-call session control function ["P-CSCF"] (350), and an external network (360). For the sake of simplicity, Figure 3 does not show lower layer bearer service functions.

In Figure 3, the gateway (340) includes an IP BS manager (342), a translation (346) function, and a UMTS BS manager (348). The IP BS manager (342) manages the inter-working with the external network (360), using mechanisms such as DiffServ Edge, RSVP/multiserv signaling, policy control, or service agreement functions. The IP BS manager (342) communicates with the UMTS BS manager (348) through the translation (346) function, which provides the inter-working between the mechanisms and parameters (e.g., QoS parameters) of the UMTS bearer service and those of the IP bearer service. Other frameworks are possible, for example, those including an IP BS manager and translation function in the UE (310), or those using other mechanisms for inter-working between networks.

The framework (300) can be used for policy-based admission control, in which a policy control function ["PCF"] (353) makes decisions in regard to network-based IP policy using policy information and rules. Policy information elements include, for example, addresses and authorized QoS for the IP flows of a session. The PCF (353) communicates policy information to the IP BS manager (342) in the gateway (340) across an interface. For IP Multimedia and other services, service-based local policy ["SBLP"] decisions can be applied to a bearer. SBLP decisions involve interaction between the UE (310), the gateway (340), and the P-CSCF (350).

In addition to the PCF (353), the P-CSCF (350) includes a local SIP proxy (351), which is used for SIP signaling and obtaining a SDP description of a session. The P-CSCF (350) and PCF (353) have several roles, including authorizing QoS resources for the session described in the SDP description. The P-CSCF (350)/PCF (353) can generate an authorization token for a SIP session and send the authorization token to the UE (310) by SIP message. The authorization token, for example, conforms to the IETF specification on SIP Extensions for Media Authorization.

The UE (310) makes resource reservation requests that the gateway (340) matches with authorizations from the PCF (353). For example, the UE (310)

WO 02/085055

PCT/US02/12181

8

includes the authorization token in PDP Context Activation or Modification requests along with UMTS QoS parameters. The authorization token can then be used to correlate the requests with the authorizations from the PCF (353).

The gateway (340) is the IP policy enforcement point and has several roles.

- 5 It controls access to QoS for flow(s) of IP packets. Policy information is either "pushed" to the gateway (340) by the PCF (353) or requested from the PCF (353) by the gateway (340). The gateway (340) also provides flow control/gating functionality, and takes action when the IP packets for a flow exceed authorization.

- 10 For additional information about Figure 3 and the service and components referenced therein, see 3G TS 23.207 v1.2.0 and related specifications.

- In general, per-flow authorization gives finer control over authorization, QoS management, and charging than per-session authorization, which in turn has advantages compared to network-level authorization alone. The authorization token generated during SIP signaling, however, is inadequate for individually identifying multiple different flows of a session for authorization.

SUMMARY

- The present invention relates to a binding mechanism for packet media flows. The binding mechanism uses an authorization token and packet media flow identifiers to identify packet media flows of a session for authorization. This provides the advantages of using a per-session authorization token while also allowing resource authorization and allocation on the basis of individual packet media flows of the session. The binding mechanism includes various aspects.

- 25 According to a first aspect, an apparatus transmits one or more messages including binding information for authorizing one or more packet media flows of a session. The binding information includes an authorization token that, when combined with a packet media flow identifier, is sufficient to identify a packet media flow of the session. For example, a UE transmits one or more PDP context requests including binding information. The binding information includes a SIP media authorization token and one or more IP media flow identifiers.

- 30 According to a second aspect, a network node processes binding information for authorizing one or more packet media flows of a session. The binding information includes an authorization token. The network node interprets each of one or more packet media flow identifiers relative to the authorization token

WO 02/085055

PCT/US02/12181

9

to identify a packet media flow of the session. For example, binding information includes a SIP media authorization token and one or more IP media flow identifiers.

Additional features and advantages of the invention will be made apparent from the following detailed description of described embodiments that proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram of a bearer service layered architecture according to the prior art.

Figure 2 is a diagram of a simplified example of a network architecture according to the prior art.

Figure 3 is a diagram illustrating QoS management functions for end-to-end IP QoS according to the prior art.

Figure 4 is a block diagram of a suitable computing environment in which described embodiments may be implemented.

Figures 5 and 6 are flowcharts of techniques for a binding mechanism using an authorization token and IP media flow identifier(s).

DETAILED DESCRIPTION

Described embodiments of the present invention are directed to a binding mechanism for authorizing QoS requested for one or more IP media flows of a session. Binding information transmitted from UE to a GGSN includes a SIP media authorization token. The GGSN interprets one or more IP media flow identifiers relative to the SIP media authorization token to identify the one or more IP media flows of the session. In terms of transmission bandwidth, computational complexity, and signaling complexity, using a per-session authorization token is more efficient than using a different authorization token per IP media flow of the session. At the same time, using multiple IP media flow identifiers in conjunction with the per-session authorization token provides a simple mechanism for resource authorization and allocation on the basis of individual IP media flows of the session.

In the described embodiments, the binding mechanism includes several techniques and systems. While the techniques and systems are typically described herein as part of a single, integrated framework, the techniques and systems can be applied separately, potentially in combination with other techniques and systems.

WO 02/085055

PCT/US02/21181

10

In the described embodiments, the binding mechanism is part of a system that complies with a variety of technical specifications, including most notably 3G TS 23.207, but also including 3G TS 23.107, 3G TS 23.060, and the IETF Internet Draft entitled "SIP Extensions for Media Authorization." In alternative embodiments,

5 the binding mechanism works in other systems and/or with other protocols.

Table 2 lists some acronyms and abbreviations used in the present application.

Short Form	Full Term
3G TS	3 rd Generation Technical Specification
3GPP	3 rd Generation Partnership Project
APN	Access Point Name
BS	Bearer Service
DiffServ	Architecture for Differentiated Services
DSCP	DiffServ Codepoint
CGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IETF	Internet Engineering Task Force
IntServ	Integrated Services in the Internet Architecture
IP	Internet Protocol
P-CSCF	Proxy - Call Session Control Function
PCF	Policy Control Function
PDA	Personal Digital Assistant
PDP	Packet Data Protocol
QoS	Quality of Service
RFC	Request for Comment
RSVP	Resource Reservation Protocol
SBLP	Service-based Local Policy
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
UA	User Agent
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network

Table 2: Acronyms and abbreviations

10

I. Computing Environment

Figure 4 illustrates a generalized example of a suitable computing environment (400) in which the described embodiments may be implemented. The computing environment (400) is not intended to suggest any limitation as to scope of use or functionality of the invention. The present invention may be implemented in diverse general-purpose or special-purpose computing environments such as cellular devices or other user equipment, or CGSN or other network nodes.

15

WO 02/085055

PCT/US02/2181

11

With reference to Figure 4, the computing environment (400) includes at least one processing unit (410) and memory (420). In Figure 4, this most basic configuration (430) is included within a dashed line. The processing unit (410) executes computer-executable instructions and may be a real or a virtual processor. In a multi-processing system, multiple processing units execute computer-executable instructions to increase processing power. The memory (420) may be volatile memory (e.g., registers, cache, RAM), non-volatile memory (e.g., ROM, EEPROM, flash memory, etc.), or some combination of the two. The memory (420) stores software (480) implementing the binding mechanism with an authorization token and flow identifier(s).

A computing environment may have additional features. For example, the computing environment (400) includes storage (440), one or more input devices (450), one or more output devices (460), and one or more communication connections (470). An interconnection mechanism (not shown) such as a bus, controller, or network interconnects the components of the computing environment (400). Typically, operating system software (not shown) provides an operating environment for other software executing in the computing environment (400), and coordinates activities of the components of the computing environment (400).

The storage (440) may be removable or non-removable, and includes magnetic disks, magnetic tapes or cassettes, CD-ROMs, CD-RWs, DVDs, or any other medium which can be used to store information and which can be accessed within the computing environment (400). The storage (440) may store computer-executable instructions for the software (480) implementing the binding mechanism with an authorization token and flow identifier(s).

The input device(s) (450) may be a touch input device such as a numerical keypad, keyboard, mouse, pen, or trackball, a voice input device, a scanning device, or another device that provides input to the computing environment (400). The output device(s) (460) may be a display, printer, speaker, CD-writer, or another device that provides output from the computing environment (400).

The communication connection(s) (470) enable communication over a communication medium to another computing entity. The communication medium conveys information such as computer-executable instructions, audio or video information, or other data in a modulated data signal. A modulated data signal is a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation,

WO 02/085055

PCT/US02/12181

12

communication media include wired or wireless media implemented with a radio frequency, electrical, optical, infrared, acoustic, or other carrier.

The invention can be described in the general context of computer-readable media. Computer-readable media are any available media that can be accessed within a computing environment. By way of example, and not limitation, with the computing environment (400), computer-readable media include memory (420), storage (440), communication media, and combinations of any of the above.

The invention can be described in the general context of computer-executable instructions, such as those included in program modules, being executed in a computing environment on a target real or virtual processor. Generally, program modules include routines, programs, libraries, objects, classes, components, data structures, etc. that perform particular tasks or implement particular abstract data types. The functionality of the program modules may be combined or split between program modules as desired in various embodiments. Computer-executable instructions for program modules may be executed within a local or distributed computing environment.

For the sake of presentation, the detailed description uses terms like "request," "generate," and "modify" to describe computer operations in a computing environment. These terms are high-level abstractions for operations performed by a computer, and should not be confused with acts performed by a human being. The actual computer operations corresponding to these terms vary depending on implementation.

II. Binding Mechanism

A binding mechanism described herein associates a PDP context bearer with policy information in a GGSN to support SBLP enforcement and QoS interworking. The policy information in the GGSN is based on IP media flows. The binding mechanism identifies the IP media flow(s) associated with a PDP context bearer and uses this identification information in selecting the policy information to apply.

For the binding mechanism, binding information (e.g., an authorization token and flow identifier(s)) provided by a UE is sufficient to identify the IP media flow(s) carried on a PDP context. The binding mechanism provides a simple mechanism that allows for resource authorization and allocation on the basis of IP media flows while retaining a single authorization token in SIP signaling and PDP context

WO 02/085055

PCT/US02/12181

13

activation/modification messages. This achieves the advantages of using a single per-session authorization token and the advantages of per-flow resource authorization and allocation.

For the policy information, for example, the P-CSCF/PCF uses an SDP description of a session to calculate authorization for the session, including restrictions on IP resources, IP packet flows, and (potentially) IP destinations. An authorized session may include one or more flow authorizations, with each flow authorization containing an IP flow 5-tuple (i.e., source address and port, destination address and port, protocol) for the flow, a specification of authorized resources for the flow, and a DSCP that identifies an assigned DiffServ per hop behavior for the flow.

IP policy enforcement is based on IP media flows, while UMTS bearers are based on PDP contexts from a UE to a GGSN. When a PDP context is activated or modified and SBLP is in effect, the GGSN uses policy information associated with IP media flows to authorize the bearer. The UE controls the mapping of IP media flows to PDP contexts, and the UE provides the GGSN with binding information to allow it to correctly identify the policy information for PDP context activation/modification request messages. Otherwise, the GGSN will not have sufficient information to identify the policy information needed to authorize the bearer.

The IETF SIP Working Group has considered using an authorization token per IP media flow in an SDP description, which could then be provided by the UE to the GGSN as binding information. While architecturally correct, this approach requires changing SDP and sending more information between the PCF, GGSN, and UE.

In contrast, for the binding mechanism described herein, IP media flows are identified by their order in an SDP description. For example, the first media flow (identified by a line beginning with "m=" in the SDP description) is flow 1, the second media flow is flow 2, etc. Since both the P-CSCF/PCF and UE have the SDP description, they will identify flows in a consistent manner. Authorization information from the P-CSCF/PCF and binding information from the UE can both identify the media flow or flows.

Figures 5 and 6 show techniques (500, 600) for a binding mechanism using an authorization token and IP media flow identifier(s). Figures 5 and 6 generally

WO 02/085055

PCT/US02/12181

14

illustrate the timing for the binding mechanism; the actual timing depends on the underlying protocols (e.g., SIP and PDP), network, etc.

With reference to Figures 5 and 6, during SIP signaling, the P-CSCF/PCF transmits (610) an authorization token and SDP description to the UE. The UE receives (510) the authorization token and SDP description.

The UE then transmits (520) a PDP context request. When activating/modifying a PDP context, the UE includes the authorization token as binding information in the request. To map media flows to PDP contexts correctly, the UE should also include one or more flow identifiers according to the SDP description. (The authorization token was sent (610) by the P-CSCF/PCF to the UE during SIP signaling, and the flow identifiers were derived by the UE according to the sequence of media flows in the SDP.) A flow identifier only needs a small number of bits, so there will be minimal impact on airlink performance. Specifically, binding information is included in PDP Context Activation/Modification messages to associate the PDP context bearer with policy information. The PDP Configuration Options parameter (an optional parameter signalled in a PDP Context Activation/Modification request) is used for this purpose. Alternatively, another parameter is used, such as a Traffic Flow Template parameter of a PDP context.

The authorization token is unique across PDP contexts associated with an APN, and conforms to the IETF specification on SIP Extensions for Media Authorization.

The flow identifiers identify the IP media flows associated with the SIP session. As described above, flow identifiers may be based on the ordering of media flows in the SDP description. In this case, a flow identifier combined with the authorization token is sufficient to uniquely identify an IP media flow, since flow identifiers are interpreted relative to an authorization token.

In order to allow QoS and policy information to be "pulled" from the PCF, the authorization token may also allow the GGSN to determine the address of the PCF to be used.

The GGSN receives (620) the PDP context request and processes the PDP context request. For example, the GGSN identifies (630) the IP media flow(s) associated with the PDP context bearer using the included binding information, queries (640) the PCF for the policy information to apply to the IP media flow(s) identified by the binding information, and uses received policy information

WO 02/085055

PCT/US02/12181
PCT/US/02/12181

15

associated with the IP media flow(s) to authorize (650) the bearer, if appropriate in view of the policy information.

5 SIP session modification can result in changes to the SDP description, such as the addition or deletion of media flows. (For example, in one implementation, when a media flow is deleted, the corresponding "m" line is still in SDP description, which will be set to "m=0". The corresponding authorized QoS resource for this deleted flow is set to zero in the PCF. When a new media flow is added, it is added at the end of the existing SDP description.) The P-CSCF/PCF may issue a new authorization token when the SDP description changes. If the resources associated with a PDP context increase as a result of the SIP session modification, the UE sends a PDP context modification with the old (or new) authorization token and flow identifiers.

15 Having described and illustrated the principles of my invention with reference to certain described embodiments, it will be recognized that the described embodiments can be modified in arrangement and detail without departing from such principles. It should be understood that the programs, processes, or methods described herein are not related or limited to any particular type of computing environment, unless indicated otherwise. Various types of general purpose or specialized computing environments may be used with or perform operations in accordance with the teachings described herein. Elements of the described embodiments shown in software may be implemented in hardware and vice versa.

20 In view of the many possible embodiments to which the principles of my invention may be applied, I claim as my invention all such embodiments as may come within the scope and spirit of the following claims and equivalents thereto.

WO 02/085055

PCT/US02/12181

16

CLAIMS

I claim:

1. In an apparatus, a method of requesting resource authorization comprising:
transmitting one or more PDP context requests including binding information for
one or more IP media flows of a session, wherein the binding information includes an
authorization token and one or more IP media flow identifiers.
2. The method of claim 1 wherein the one or more IP media flow identifiers
combine with the authorization token to identify the one or more IP media flows.
3. The method of claim 1 wherein the apparatus is user equipment, and
wherein the one or more IP media flow identifiers reference a flow order in a SDP
description that is accessible to the user equipment and a P-CSCF/PCF.
4. The method of claim 1 wherein each PDP context request is a PDP context
activation request or a PDP context modification request.
5. A computer-readable medium having encoded therein computer-executable
instructions for causing a computer programmed thereby to perform the method of
claim 1.
6. In a network node, a method of authorizing resources comprising:
processing binding information for one or more IP media flows of a session,
wherein the binding information includes an authorization token and one or more IP
media flow identifiers.
7. The method of claim 6 wherein the one or more IP media flow identifiers
combine with the authorization token to identify the one or more IP media flows.
8. The method of claim 6 wherein the network node comprises a P-CSCF/PCF,
and wherein the one or more IP media flow identifiers reference a flow order in a SDP
description that is accessible to the P-CSCF/PCF and user equipment.

WO 02/48505

PCT/US02/12181

17

9. The method of claim 6 wherein the processing comprises authorizing the one or more IP media flows according to a service-based local policy decision.

5 10. A computer-readable medium having encoded therein computer-executable instructions for causing a computer programmed thereby to perform the method of claim 6.

11. A computer-readable medium having encoded therein computer-executable instructions for causing user equipment programmed thereby to perform a method of requesting resource authorization and allocation, the method comprising:
receiving a media authorization token; and
transmitting a context activation request including the media authorization token
for authorizing each of one or more media flows of a session, wherein the media
15 authorization token in combination with a media flow identifier from among plural media flow identifiers is sufficient to uniquely identify a media flow from among plural media flows of the session.

12. The computer-readable medium of claim 11 wherein the plural media flow identifiers reference a flow order in a session description, and wherein a gateway node
20 authorizes the one or more media flows according to a service-based local policy decision.

13. The computer-readable medium of claim 11 wherein the method further
25 comprises:
receiving a second media authorization token; and
transmitting a context modification request including the second media authorization token for modifying authorization of the one or more media flows.

14. A computer-readable medium having encoded therein computer-executable instructions for causing a network node programmed thereby to perform a
30 method of authorizing and allocating resources, the method comprising:

- receiving a context request including a media authorization token for authorizing each of one or more media flows of a session, wherein the media authorization token in combination with a media flow identifier from among plural media flow identifiers is sufficient to uniquely identify a media flow from among plural media flows of the session; and
- 5 requesting policy information indicated by the media authorization token.
15. The computer-readable medium of claim 14 wherein the plural media flow identifiers reference a flow order in a session description.
- 10 18. The computer-readable medium of claim 14 wherein the method further comprises:
- authorizing the one or more media flows according to a service-based local policy decision.
- 15 17. A computer-readable medium having encoded therein computer-executable instructions for causing user equipment programmed thereby to perform a method of requesting resource authorization and allocation for one or more packet media flows of a session, the method comprising:
- 20 receiving an authorization token and packet media flow information during session protocol signaling, the packet media flow information accessible to a network node and the user equipment; and
- transmitting one or more messages including binding information for authorizing one or more packet media flows of a session, wherein the binding information includes the authorization token, whereby each of one or more packet media flow identifiers is interpreted relative to the authorization token to identify a packet media flow of the session.
- 25 18. The computer-readable medium of claim 17 wherein the user equipment is a cellular device, wherein the network node comprises a GGSN, and wherein each of the one or more messages is a PDP context activation or modification request.
- 30
-

WO 02/085055

PCT/US02/12181

19

19. The computer-readable medium of claim 17 wherein the one or more packet media flows are IP media flows.
20. The computer-readable medium of claim 17 wherein a SDP description
5 comprises the packet media flow information, and wherein the one or more packet media flow identifiers reference a media order in the SDP description.
21. The computer-readable medium of claim 17 wherein the session protocol is SIP, and wherein a PCF of a P-CSCF generates the authorization token.
10
22. The computer-readable medium of claim 17 wherein the user equipment transmits a single message to request resource authorization and allocation for all packet media flows of the session.
- 15 23. A computer-readable medium having encoded therein computer-executable instructions for causing a network node programmed thereby to perform a method of authorizing and allocating resources for one or more packet media flows of a session, the method comprising:
transmitting an authorization token and packet media flow information during
20 session protocol signaling, the packet media flow information accessible to the network node and user equipment;
processing one or more messages including binding information for authorizing one or more packet media flows of a session, wherein the binding information includes the authorization token, and wherein the processing includes interpreting each of one
25 or more packet media flow identifiers relative to the authorization token to identify a packet media flow of the session.
24. The computer-readable medium of claim 23 wherein the user equipment is a cellular device, wherein the network node comprises a GGSN, and wherein the one
30 or more packet media flows are IP media flows.

WO 02/085655

PCT/US02/12181

20

25. The computer-readable medium of claim 23 wherein a SDP description comprises the packet media flow information, and wherein the one or more packet media flow identifiers reference a media order in the SDP description.

5 26. The computer-readable medium of claim 23 wherein the session protocol is SIP, and wherein a PCF of a P-CSCF generates the authorization token.

27. The computer-readable medium of claim 23 wherein the network node processes a single message requesting resource authorization and allocation for all
10 packet media flows of the session.

28. The computer-readable medium of claim 23 wherein the method further comprises:
requesting policy information indicated by the authorization token.

WO 02/085055

PCT/US02/12181

1/4

Figure 1, prior art

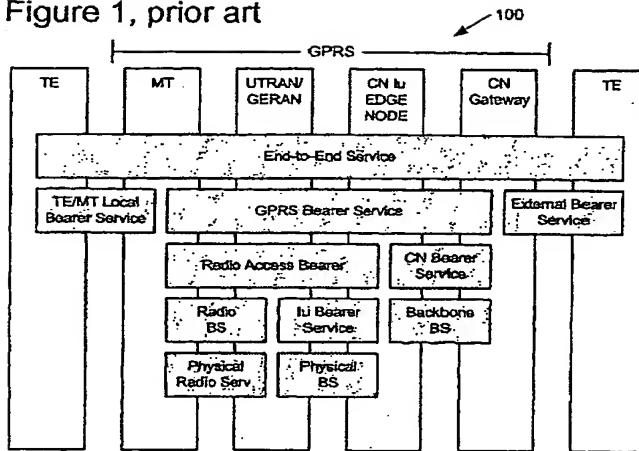


Figure 4

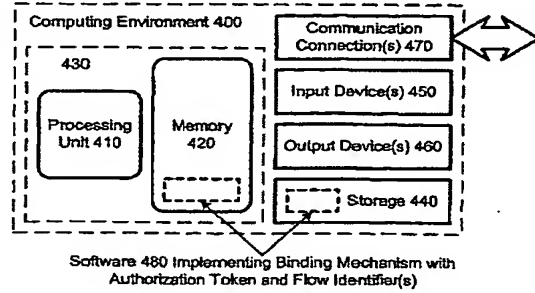


Figure 2, Prior Art

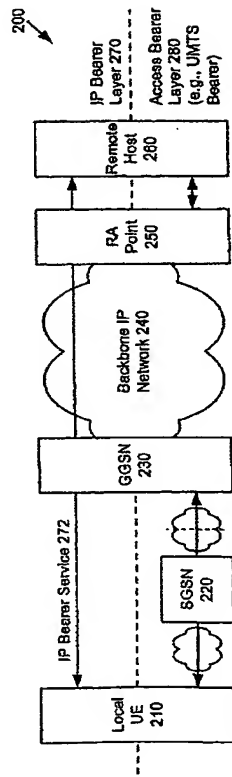
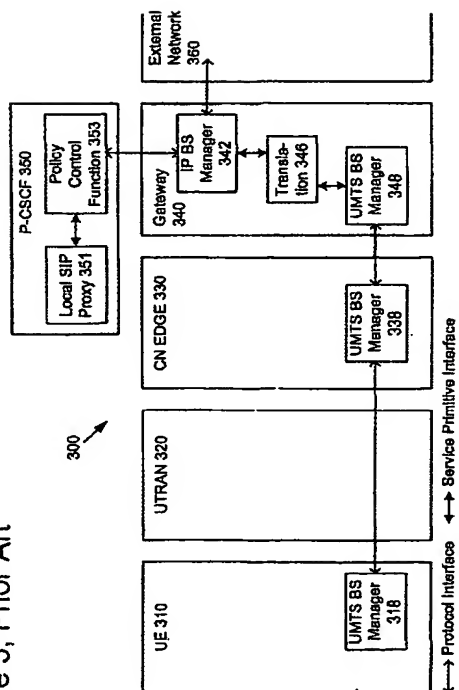


Figure 3, Prior Art



WO 02/085055

PCT/US02/2181

4/4

Figure 5

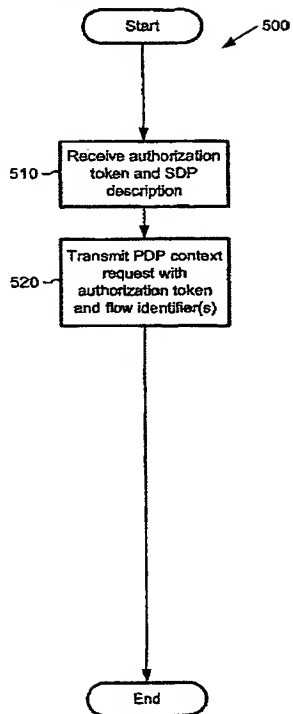
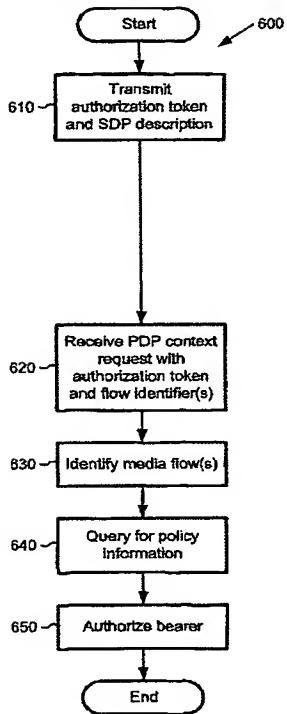


Figure 6



【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

INTERNATIONAL PATENT COOPERATION TREATY

(43) International Publication Date
24 October 2002 (24.10.2002)

PCT

(10) International Publication Number
WO 02/085055 A3(51) International Patent Classification: H04Q 7/24
H04L 12/56, 12/28(US/US): 21433 SF 33rd Place, Sammamish, WA 98075
(US).

(21) International Application Number: PCT/US02/12191

(74) Agent: RINEHART, Kyle, B., Knappton Squares, I.J.P.,
One World Trade Center, Suite 1600, 121 SW Salmon
Street, Portland, OR 97204 (US).

(22) International Filing Date: 16 April 2002 (16.04.2002)

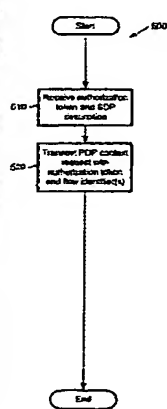
(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/284,358 17 April 2001 (17.04.2001) US
10/091,047 4 March 2002 (04.03.2002) US(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EG, ES, FI, GB, GR, GU, HK,
HM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LA,
LK, LR, LS, LV, LY, MA, MD, MG, MK, MN, MW,
MX, MY, NZ, OM, PA, PE, PG, PH, PL, PT, RO, RU, SD, SE, SG,
SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VN, YU, ZA, ZM, ZW.(71) Applicant (for all designated States except US): AT & T
WIRELESS SERVICES, INC. (US/US); 7277 164th Avenue
N.E., Redmond, WA 98052 (US).(84) Designated States (regional): ARIPO patent (GI, GM,
KE, LS, MW, MZ, NA, SZ, TZ, UG, ZM, ZW);
European patent (AM, AZ, BY, KG, KZ, MD, NL, PL, PT, RO,
RU, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VN, YU, ZA, ZM, ZW).(72) Inventor; and
(73) Inventor/Applicant (for US only): SHEEH, Hugh, W.

[Continued on next page]

(54) Title: BINDING INFORMATION FOR IP MEDIA FLOWS



(57) Abstract: A binding mechanism uses an authentication token and packet media flow identifier(s) to identify packet media flow(s) of a session for authorization. This provides the advantages of using a per-session authentication token while also allowing resource authorization and allocation on the basis of individual packet media flows of the session. The binding mechanism includes various aspects.

WO 02/085055 A3

WO 02/085055 A3

GB, GR, IL, LU, MC, NL, PT, SE, TR, OAPI patent
(HU, HU, CZ, CG, CY, DM, EA, EP, OQ, GW, ML, MR,
NT, SN, TD, TG).

(58) Date of publication of the international search report:
6 February 2005

Declaration under Rule 4.17:

— of inventorship (Rule 4.17(b)) for US only

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International Application No. PCT/US 02/12181
A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H0407/24 H04L12/56 H04L12/28		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search phase of data base used, where practical, search terms used EPO-Internal, WPI Data, PAJ, COMPENDEX		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim no.
A	WO 00 10357 A (NOKIA NETWORKS OY ; HAUMONT SERGE (FI); NIERELAE TUOMAS (FI); PUUSK) 24 February 2000 (2000-02-24) page 10, line 22 - line 30 page 13, line 15 - line 16 page 18, line 25 - page 19, line 15; figure 3	1-28
A	WO 99 05828 A (ERICSSON TELEFON AB L M) 4 February 1999 (1999-02-04) abstract page 7, line 8 - page 8, line 23 page 12, line 23 - page 13, line 17 page 18, line 1 - line 2 -/-	1-28
<input checked="" type="checkbox"/> Further documents are listed in the continuation of section C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document containing the general state of the art which is not considered to be of particular relevance "C" document cited in prior art or after the international filing date "D" document which may have doubts as to its status (claim) or which is cited to establish the priority date of another claim or other special reason (as specified) "E" document relating to an oral disclosure, use, exhibition or other means "F" document published prior to the international filing date but after the priority date claimed "I" late document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family		
Date of the latest completion of the international search		Date of mailing of the international search report
22 October 2002		04/11/2002
Name and mailing address of the ISA European Patent Office, P.O. Box 5818, Postfach 2 D-6000 Frankfurt am Main Tel. (+49-69) 940-2040, Telex 51 851 990 01 Fax: (+49-69) 940-2010		Authorized officer Mannekens, J

Form PCT/ISA/210 (continued sheet) (July 1999)

INTERNATIONAL SEARCH REPORT		International Application No. PCT/US 02/12181
C/Candidates DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with keywords, where appropriate, of the relevant passages	Relevant to claim No.
A	SINNREICH H ET AL: "INTERDOMAIN IP COMMUNICATIONS WITH QOS, AUTHORIZATION AND USAGE REPORTING" INTERNET DRAFT, XX, XX, February 2000 (2000-02), pages 1-67, XP002939495 the whole document	1-28
A	MARSHALL ET AL: "SIP Extensions for Media Authorization" INTERNET DRAFT, 'Online! February 2001 (2001-02), XP002217605 Retrieved from the Internet: <URL:http://www.watersprings.org/pub/1d/draft-ietf-sip-call-auth-01.txt> 'retrieved on 2002-10-22! cited in the application the whole document	1-28

Form PCT/SGA/210 (Specification of relevant documents) (July 2002)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.
PCT/US 02/12181

FCI/DS 02/12181

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0010357	A	24-02-2000	FI 981722 A AU 5291899 A BR 9912911 A CA 2339825 A1 CN 1317217 T EP 1104639 A1 WO 0010357 A1 JP 2002523938 T	11-02-2000 06-03-2000 08-05-2001 24-02-2000 10-10-2001 06-06-2001 24-02-2000 30-07-2002
WO 9905828	A	04-02-1999	AU 739717 B2 AU 8369898 A BR 9810796 A CN 1271488 T EP 0997018 A1 NZ 502339 A NO 9905828 A1	18-10-2001 16-02-1999 25-07-2000 25-10-2000 03-05-2000 30-11-2001 04-02-1999

Form PCT/ISPC/210 (Revised family search) (July 1999)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT, BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN, TD,TC),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE, GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,P L,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZM,ZW

(74)代理人 100096013

弁理士 富田 博行

(74)代理人 100120112

弁理士 中西 基晴

(72)発明者 シェー, ヒュー・エイチ

アメリカ合衆国ワシントン州98075, サマミッシュ, サウスイースト・サーティサード・ブレ
イス 21433

Fターム(参考) 5K030 GA11 HA08 HB13 HC09 JL01 JT09 KA01 KA02 LB02 LC01

5K067 AA11 BB21 DD11 DD17 EE02 EE10 EE16 HH22 HH23 HH24

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第7部門第3区分
 【発行日】平成17年12月22日(2005.12.22)

【公表番号】特表2004-533160(P2004-533160A)
 【公表日】平成16年10月28日(2004.10.28)
 【年通号数】公開・登録公報2004-042
 【出願番号】特願2002-582649(P2002-582649)
 【国際特許分類第7版】

H 0 4 L 12/56

H 0 4 Q 7/36

H 0 4 Q 7/38

【F I】

H 0 4 L 12/56 2 0 0 A

H 0 4 B 7/26 1 0 9 M

H 0 4 B 7/26 1 0 5 D

【手続補正書】

【提出日】平成17年4月15日(2005.4.15)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

装置において、リソース許可を要求する方法であって、

セッションの1つ以上のIPメディア・フローについてのバインド情報を含む1つ以上のPDPコンテキスト要求を送信するステップを含み、前記バインド情報が、許可トークンと、1つ以上のIPメディア・フロー識別子とを含む、方法。

【請求項2】

請求項1記載の方法において、前記1つ以上のIPメディア・フロー識別子は、前記許可トークンと組み合わせて、前記1つ以上のIPメディア・フローを特定する、方法。

【請求項3】

請求項1記載の方法において、前記装置はユーザ機器であり、前記1つ以上のIPメディア・フロー識別子は、前記ユーザ機器およびP-CSCF/PCFにアクセス可能なSDP記述におけるフローの順序を参照する、方法。

【請求項4】

請求項1記載の方法において、各PDPコンテキスト要求は、PDPコンテキスト活性化要求またはPDPコンテキスト変更要求である、方法。

【請求項5】

コンピュータ実行可能命令がエンコードされたコンピュータ読み取り可能媒体であって、これによってプログラムされたコンピュータに、請求項1記載の方法を実行させる、コンピュータ読み取り可能媒体。

【請求項6】

ネットワーク・ノードにおいて、リソースを許可する方法であって、セッションの1つ以上のIPメディア・フローについてのバインド情報を処理するステップを含み、前記バインド情報が、許可トークンと、1つ以上のIPメディア・フロー識別子とを含む、方法。

【請求項7】

請求項 6 記載の方法において、前記 1 つ以上の IP メディア・フロー識別子は、前記許可トークンと組み合わせて、前記 1 つ以上の IP メディア・フローを特定する、方法。

【請求項 8】

請求項 6 記載の方法において、前記ネットワーク・ノードは P-CSCF/PCF を備え、前記 1 つ以上の IP メディア・フロー識別子は、前記 P-CSCF/PCF およびユーザ機器にアクセス可能な SDP 記述におけるフローの順序を参照する、方法。

【請求項 9】

請求項 6 記載の方法において、前記処理するステップは、サービスに基づく個別ポリシー判断に応じて前記 1 つ以上の IP メディア・フローを許可することを含む、方法。

【請求項 10】

コンピュータ実行可能命令がエンコードされたコンピュータ読み取り可能媒体であって、これによってプログラムされたコンピュータに、請求項 6 記載の方法を実行させる、コンピュータ読み取り可能媒体。

【請求項 11】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたユーザ機器に、リソース許可および配分を要求する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

メディア許可トークンを受信するステップと、

セッションの 1 つ以上のメディア・フローの各々を許可するための前記メディア許可トークンを含むコンテキスト活性化要求を送信するステップと、
を含み、前記メディア許可トークンと、複数のメディア・フロー識別子からのメディア・フロー識別子との組み合わせが、前記セッションの複数のメディア・フローの中からメディア・フローを一意に特定するのに十分である、コンピュータ読み取り可能媒体。

【請求項 12】

請求項 11 記載のコンピュータ読み取り可能媒体において、前記複数のメディア・フロー識別子は、セッション記述におけるフローの順序を参照し、ゲートウェイ・ノードが、サービスに基づく個別ポリシー判断に応じて前記 1 つ以上のメディア・フローを許可する、コンピュータ読み取り可能媒体。

【請求項 13】

請求項 11 記載のコンピュータ読み取り可能媒体において、前記方法は、更に、

第 2 メディア許可トークンを受信するステップと、

前記 1 つ以上のメディア・フローの許可を変更するため、前記第 2 メディア許可トークンを含むコンテキスト変更要求を送信するステップと、
を含む、方法。

【請求項 14】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたネットワーク・ノードに、リソースを許可し配分する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

セッションの 1 つ以上のメディア・フローの各々を許可するためのメディア許可トークンを含むコンテキスト要求を受信するステップであって、前記メディア許可トークンと、複数のメディア・フロー識別子からのメディア・フロー識別子との組み合わせが、前記セッションの複数のメディア・フローの中からメディア・フローを一意に特定するのに十分である、ステップと、

前記メディア許可トークンが示すポリシー情報を要求するステップと、
を含むコンピュータ読み取り可能媒体。

【請求項 15】

請求項 14 記載のコンピュータ読み取り可能媒体において、前記複数のメディア・フロー識別子は、セッション記述におけるフローの順序を参照する、方法。

【請求項 16】

請求項 14 記載のコンピュータ読み取り可能媒体において、前記方法は、更に、

サービスに基づく個別ポリシー判断に応じて、前記1つ以上のメディア・フローを許可するステップを含む、方法。

【請求項17】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたユーザ機器に、セッションの1つ以上のパケット・メディア・フローについてリソースの許可および配分を要求する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

セッション・プロトコルの通知の間に、許可トークンおよびパケット・メディア・フロー情報を受信するステップであって、前記パケット・メディア・フロー情報が、ネットワーク・ノードおよび前記ユーザ機器にアクセス可能である、ステップと、

セッションの1つ以上のパケット・メディア・フローを許可するためにバインド情報を含む1つ以上のメッセージを送信するステップであって、前記バインド情報が前記許可トークンを含むことにより、1つ以上のメディア・フロー識別子の各々を、前記許可トークンに関して解釈して、前記セッションのパケット・メディア・フローを特定する、ステップと、

を含む、コンピュータ読み取り可能媒体。

【請求項18】

請求項17記載のコンピュータ読み取り可能媒体において、前記ユーザ機器はセルラ・デバイスであり、前記ネットワーク・ノードはGGSNから成り、前記1つ以上のメッセージの各々は、PDPコンテキスト活性化または変更要求である、コンピュータ読み取り可能媒体。

【請求項19】

請求項17記載のコンピュータ読み取り可能媒体において、前記1つ以上のパケット・メディア・フローはIPメディア・フローである、コンピュータ読み取り可能媒体。

【請求項20】

請求項17記載のコンピュータ読み取り可能媒体において、前記SDP記述は、前記パケット・メディア・フロー情報を含み、前記1つ以上のパケット・メディア・フロー識別子は、前記SDP記述におけるメディアの順序を参照する、コンピュータ読み取り可能媒体。

【請求項21】

請求項17記載のコンピュータ読み取り可能媒体において、前記セッション・プロトコルはSIPであり、P-CSCFのPCFが前記許可トークンを生成する、コンピュータ読み取り可能媒体。

【請求項22】

請求項17記載のコンピュータ読み取り可能媒体において、前記ユーザ機器は、単一のメッセージを送信して、前記セッションの全てのパケット・メディア・フローについてのリソース許可および配分を要求する、コンピュータ読み取り可能媒体。

【請求項23】

コンピュータ実行可能命令がエンコードされ、これによってプログラムされたネットワーク・ノードに、セッションの1つ以上のパケット・メディア・フローに対してリソースを許可および配分する方法を実行させる、コンピュータ読み取り可能媒体であって、前記方法が、

セッション・プロトコルの通知の間に、許可トークンおよびパケット・メディア・フロー情報を送信するステップであって、前記パケット・メディア・フロー情報が、前記ネットワーク・ノードおよびユーザ機器にアクセス可能である、ステップと、

セッションの1つ以上のパケット・メディア・フローを許可するためにバインド情報を含む1つ以上のメッセージを処理するステップであって、前記バインド情報が前記許可トークンを含み、前記処理が、1つ以上のパケット・メディア・フロー識別子の各々を前記許可トークンに関して解釈して、前記セッションのパケット・メディア・フローを特定することを含む、ステップと、

を備えたコンピュータ読み取り可能媒体。

【請求項 2 4】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記ユーザ機器はセルラ・デバイスであり、前記ネットワーク・ノードは G G S N から成り、前記 1 つ以上のパケット・メディア・フローは I P メディア・フローである、コンピュータ読み取り可能媒体。

【請求項 2 5】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、S D P 記述が前記パケット・メディア・フロー情報を含み、前記 1 つ以上のメディア・フロー識別子が前記 S D P 記述におけるメディアの順序を参照する、コンピュータ読み取り可能媒体。

【請求項 2 6】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記セッション・プロトコルは S I P であり、P - C S C F の P C F が前記許可トークンを生成する、コンピュータ読み取り可能媒体。

【請求項 2 7】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記ネットワーク・ノードは、前記セッションの全てのパケット・メディア・フローに対するリソースの許可および配分を要求する単一のメッセージを処理する、コンピュータ読み取り可能媒体。

【請求項 2 8】

請求項 2 3 記載のコンピュータ読み取り可能媒体において、前記方法が、更に、前記許可トークンが示すポリシー情報を要求するステップを含む、コンピュータ読み取り可能媒体。